Utnyttjande av uppkopplingssekvenser för att ansluta enheter till falska anslutningspunkter

Jesper Winsten 41051
Kandidatavhandling i datavetenskap
Handledare: Kristian Nybom
Fakulteten för naturvetenskap och teknik
Åbo Akademi
31 mars 2020

Referat

Detta är min abstrakt som berättar om vad avhandlingen skall behandla.

Innehåll

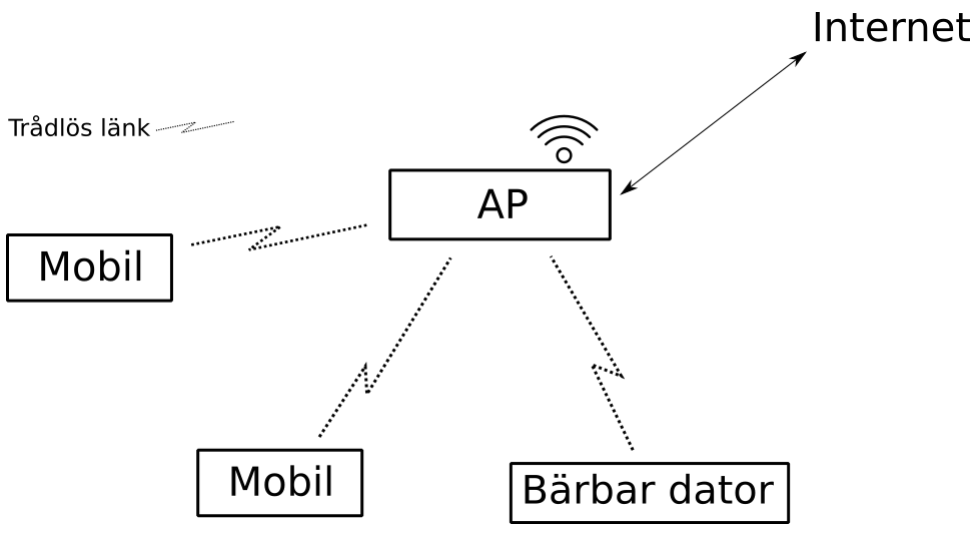
1 Introduktion

Det som i lekmannatermer kallas för Wifi är något som i dagens läge används av majoriteten av människor för att koppla upp till internet. Arbetstermen för WiFi är 802.11 som är en samling av standarder för trådlösa datornätverk. WiFi-nätverk finns överallt och är i många fall öppna för allmänheten. På grund av att nätverken är öppna för vem som helst och för att WiFi-standarden har vissa brister i säkerheten när klienter och nätverk ansluter sig till varandra, leder det till att tredje parter kan ta nytta av dessa kryphål. WiFi använder sig av flera olika topologier men den som tas mest upp i denna avhandling är infrastrukturbaserade nätverk som innehåller en anslutningspunkt vilken alla klienter ansluts till för att sedan kunna anslutas till internet. 802.11 har sedan 1997 som den första grundstandardenpublicerades utvecklats i en ständig takt. Standarderna 802.11a och 802.11b var egentligen de första standarderna som hade en omfattande implementering övre hela världen med hastigheter som nådde upp till 54 Mb/s och en säkerhetsstandard som nu är föråldrad och väldigt osäker; alltså WEP. Ända tills nutid var man använder sig av 802.11ac med en ökad hastighet upp till 3466 Mb/s och en förstärkt säkerhet med WPA2 som är en uppdatering till WPA som i sin tur var en uppdatering till WEP. Dock finns det som sagt brister i denna säkerhet som kan rätt så enkelt utnyttjas diverse metoder eller attacker som man även kan kalla dem. De flesta av attackerna som kommer att förklaras i denna avhandlingen utnyttjar sättet som klienter väljer att ansluta sig till nätverk, så kallade uppkopplingssekvenser i 802.11-standarden. Bland annat används då metoder som Evil Twin och Karma attacker för att få klienter att ansluta sig till en falsk anslutningspunkt. Andra attacker missbrukar MAC-randomiseringen i MAC-protokollet för att skapa så kallade ”fingeravtryck” av klienter för att kunna spåra dem i real-tid. Så gott som alla va dessa attacker används av personer som har en skadlig avsikt som att t.ex. försöka lura personer att skriva in sina bank koder i en falsk hemsida. Metoderna kan även användas för så kallade penetrationstester som har som avsikt att hitta fel i nätverkssäkerheten för att förbättra den.

2 Allmän överblick av WiFi och dess användning

WiFi eller trådlösa lokala datornät (*eng.* wireless local area network (WLAN)) är baserade på en familj av standarder för trådlös kommunikation. WiFi-chippsatser har funnits i mobiltelefoner, datorer och diverse anslutningspunkter (AP) inom t.ex. butiker i flera år. WiFi är specifikt menat för lokala nätverk till skillnad från mobila nätverk som LTE (*eng.* Long-Term Evolution) som är baserat på GSM-teknologin (*eng.* Global System for Mobile Communications) (Dignited, u. å.). Denna avhandling kommer dock i första hand att behandla anslutningen till WiFi med hjälp av mobila telefoner.

Termen Wifi används oftast när man pratar om den teknologi som standardiserats av the Institute of Electrical and Electronics Engineers (IEEE) under 802.11 som är en samling av standarder för WLAN. Själva namnet WiFi kommer från den icke vinstdrivande organisationen Wi-Fi Alliance som bedriver tester för officiella WiFi-certifierade enheter (Alliance, u. å.-a). Det finns tre olika topologier när man pratar om WiFi nätverk: infrastrukturbaserade nätverk, adhocnätverk (även kallad spontana nätverk) och meshnätverk (*eng.* Mesh network). Infrastrukturbaserade nätverk innehåller en AP som alla klienter ansluts till för att sedan anslutas till internet. Denna topologi som är illustrerad i figur 1 är den som används mest, speciellt i hemmen (Gorshe m. fl., 2014).



Figur 1: Infrastrukturbaserat nätverk.

Ad hoc-nätverk är så kallade icke-hierarkiska nätverk (*eng.* peer-to-peer network) där alla noder inom nätverket är kopplade till varandra utan en central AP. Noderna är vanligen mobiltelefoner eller bärbara datorer. Bluetooth är en av teknologierna som kan användas för att kommunicera via ad hoc-nätverk (Suri & Rani, 2007). Meshnätverk påminner om ad hoc-nätverk förutom att alla noder är kopplade till sina närmaste grannar istället för att alla noder är kopplade till varandra. Tanken är att oavsett avståndet mellan noder så kan man koppla dem till varandra med ett eller flera "hopp". Ett "hopp"i detta fall är när meddelanden flyttar sig mellan noderna ända tills det når sin slutgiltiga destination (Akyildiz & Xudong Wang, 2005).

3 WiFi-standarderna (IEEE 802.11)

Gruppen vars uppgift det var att definiera de diverse standarderna för lokala datornät (*eng.* Local Area Networks, LAN) uppstod år 1980 under namnet Project 802. Standarderna som Project 802 definierade omfattar bland annat datalänklagret (*eng.* Data Link Layer) och det fysiska lagret (*eng.* Physical Layer) som nu används av *the International Organization for Standardization* (ISO) *open system interconnection* (OSI) sju lagers referensmodell; den så kallade OSI-modellen (Holt & Huang, 2010). Denna avhandling kommer främst att gå igenom datalänklagret eller mera specifikt en av dess underlager; Media Access Control (MAC).

3.1 Evolutionen av 802.11

Ursprungs standarden 802.11 som publicerades 1997 är standarden som alla efterkommande WiFi standarder är baserade på. Standarder som har utvecklas och ännu också utvecklas är förbättringar på denna standard. Dessa standarder namnges med en liten bokstav efter namnet på originalstandarden, t.ex. 802.11b. Förbättringarna har i största drag fokuserat på att förbättra prestandan samt säkerheten på nätverk. 802.11 standarden hade en hastighet på 1-2 Mb/s över 2.4 Ghz frekvensen.

År 1999 förbättrades standarden kraftigt när 801.11a och 802.11b publicerades. 802.11b använde sig av samma frekvens som originalstandarden men medförde en höjd hastighet på 5.5-11 Mb/s. 802.11b införde även kryptografisk säkerhet, *wired equivalent privacy* (WEP) för att öka säkerheten. 802.11a använder sig av 5Ghz

frekvensen för att uppnå en ökad prestanda som går up till 54 Mb/s men kan även anpassa hastigheten enligt tabell 1.

År 2003 publicerades 802.11g som kombinerade det bästa från 802.11a och 802.11b standarderna med att använda sig av modulationsmetoden Ortogonal frekvensdelningsmultiplexering (OFDM) som redan användes i 802.11a. OFDM delar informationen i flera parallella dataströmmar som moduleras enskilt. En fördel med OFDM är hanteringen av störningar som endast drabbar vissa frekvenser (Electronics Notes, u. å.). På grund av diverse säkerhetsrisker med WEP som gjorde att säkerheten till nätverk kunde kringgås väldigt enkelt så skapades standarden 802.11i. 802.11i publicerades 2004 med *WiFi Protected Access II* (WPA2) för att lösa problemen med säkerheten.

År 2009 publicerades 802.11n standarden med *multiple input multiple output* (MIMO) teknologin. Med hjälp av MIMO kan nätverk använda sig av flera sändar- och mottagarantenner på samma frekvens för ökad prestanda (Intel Corporation, 2019). 802.11n kan använda sig av antingen 2.4 eller 5 Ghz frekvenserna. Beroende på vilken frekvens som används så kan nätverket nå en hastighet up till 288.8 Mb/s med 2.4 Ghz eller up till 600 Mb/s med 5 Ghz (Holt & Huang, 2010).

Standarden 802.11ac publicerades i två iterationer (Alliance, u. å.-b). Första iterationen var Wave 1 som publicerades 2013 som en uppdatering till 802.11n standarden. 802.11ac Wave 1 använder sig av 5 Ghz frekvensen med en ökad bandbredd på 80 Mhz. Wave 1 har en prestanda på 1733 Mb/s medan den 2016 steg upp till 3466.8 Mb/s när Wave 2 släpptes. Wave 2 ökade bandbredden ytterligare med en 160 Mhz kanal. Wave 2 kom även med en uppdatering till MIMO teknologin, nämligen *Multiple User Multiple Input Multiple Output* (MU-MIMO) (SecureEdge, 2016; Gast, 2013).

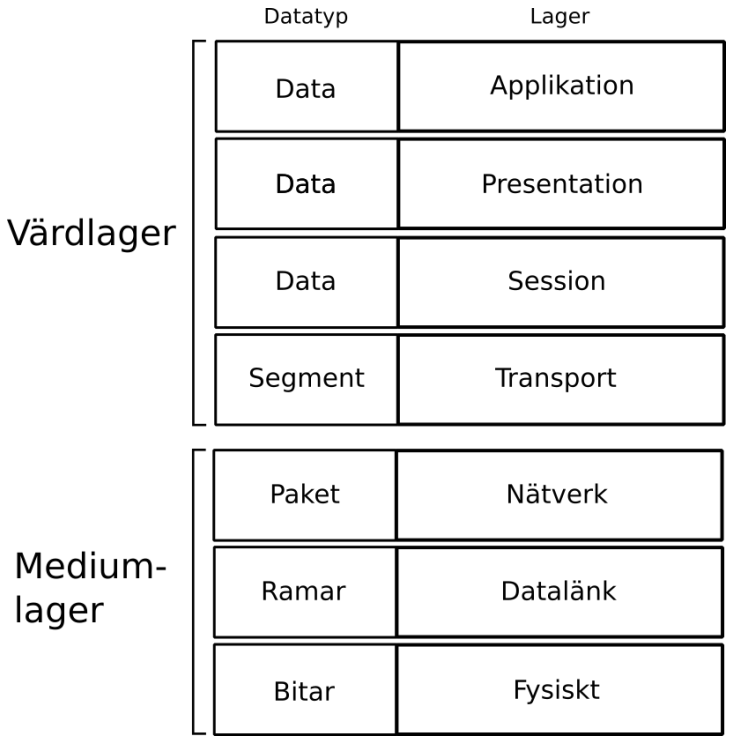
Alla standarder är bakåtkompatibla, t.ex. om en klient på ett 802.11ac nätverk inte kan använda sig av 802.11ac standarden så använder sig klienten av en tidigare standard, som i detta fall skulle vara 802.11n. För en överblick av standarderna hänvisas läsaren till tabell 1.

Standard	Lansering	Frekvens (GHz)	Hastighet (Mb/s)	Säkerhet
802.11	1997	2.4	1, 2	WEP
802.11b	1999	2.4	1, 2, 5.5, 11	WEP
802.11a	1999	5	6, 9, 12, 18, 24, 36, 48, 54	WEP
802.11g	2003	2.4	6, 9, 12, 18, 24, 36, 48, 54	WPA
802.11n	2009	2.4/5	288.8, 600	WPA2
802.11ac	2016	5	up till 3466.8	WPA2

Tabell 1: 802.11 standarderna

3.2 OSI-modellen

OSI-modellen består av sju stycken lager som definierar strukturen på datornätverk. Strukturen är uppbyggd på det viset att lagren närmast till varandra skall kommunicera med varandra. Modellen illustreras i sin helhet i figur 2 där man även kan se hierarkin från det fysiska lagret till applikationslagret. Avhandligen kommer dock endast att gå i detalj igenom datalänk lagret och des underlager MAC och LLC. Mera information om OSI-modellen kan läsas från Faircloth (2014) artikel om nätverk.



Figur 2: OSI-Modellen.

3.2.1 Datalänklagret

Datalänklagret är det andra lagret i ISO modellen. Detta lager har som uppgift att upprätthålla överföringen av dataramar mellan två klienter inom samma nätverk. Mera detaljer om dataramar tas upp senare i avhandlingen. På sändarsidan tar datalänklagret in meddelanden från nätverklagret, formaterar dem till delade dataramar och översätter dem till binärt kodad information så att det fysiska lagret sedan kan överföra informationen trådlöst via t.ex. radiovågor över WiFi. Dessa dataramar har även med sig adressinformation (*eng.* header) som innehåller destinationen vart informationen skall samt från vilken hårdvaruadress informationen kom ifrån. Dataklänklagret har även andra viktiga uppgifter som att hantera felmeddelanden och flödeskontroll. Som figur 2 hänvisar till så delas datalänklagret in i två underlager: Media Access Control (MAC) och Logical Link Control (LLC) (Lammle, 2009).

MAC underlagret fungerar som ett gränssnitt mellan det fysiska lagret och LLC underlagret. MAC kontrollerar växelverkan mellan hårdvaran samt det trådlösa överföringsmediumet. Det är även på detta underlager som hårdvarans MAC-adress finns. En MAC-adress kan tänkas sig som hårdvarans namn, alltså hur den identifieras inom nätverket (Faircloth, 2014). Följande kapitel kommer att förklara MAC i mera detalj.

LLC underlagret fungerar som ett gränssnitt mellan MAC och nätverkslaget. Det är detta underlager som tar hand om dataramarna som nämndes tidigare. LLC har hand om mutliplexering av nätverksprotokoll vilket gör det möjligt att använda flera protokoll samtidigt medan man kommunicerar över något medium (Faircloth, 2014).

3.3 Uppkopplingssekvenser till WiFi-nätverk

Uppkopplingen till WiFi-nätverk fungerar lite annorlunda än för trådbaserade nätverk. Med WiFi så måste man använda så kallade uppkopplingssekvenser. Anslutningsprocessen måste utföra tre steg förrän en mobilstation, tänk dig mobiltelefon/bärbar dator tillåts att ansluta och överföra data på nätverket. Först måste mobilstationen hitta ett kompatibelt nätverk den kan ansluta sig till. Till näst så måste nätverket acceptera och autentisera anslutningen för mobilstationen. Till sist så måste mobilstationen associeras med nätverket för att få tillåtelse att överföra data över nätverket.

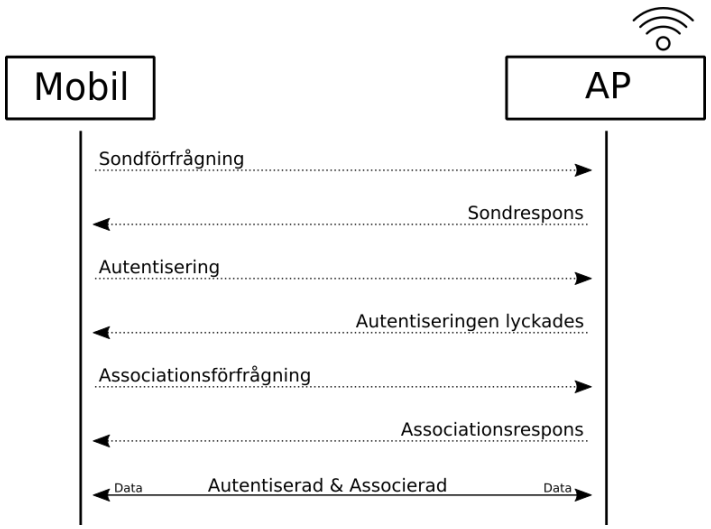
I princip så händer detta i tre olika tillstånd (*eng.* state) med hjälp av tre olika

klasser av ramar. Tillstånden är enligt följande; Initialtillståndet, alltså tillstånd ett som innebär är att mobilstationen är oautentiserad samt icke-associerad med nätverket. Tillstånd två, autentiserad men inte associerad. Tredje tillståndet, autentiserad samt associerad. Ramarna är som sagt i tre olika klasser, klasserna får endast överföra data i vissa tillstånd. Klass ett får överföra data i tillstånd ett, klass ett och två får överföra data i tillstånd två, medan alla klasser får överföra data i tillstånd tre.

Första klassens ramar används för bas operationer inom nätverket som t.ex. att skicka ut sondförfrågningar (*eng.* Probe Request) och sondresponser (*eng.* Probe Response) för att hitta nätverk. Det är även med hjälp av klass ett ramar som stationer autentiseras och därefter går upp ett steg från tillstånd ett till två. Andra klassens ramar används efter att en station har blivit autentiserad. Klass två ramar tar sedan hand om associationen mellan stationen och nätverket som sedan flyttar stationen vidare ett steg från tillstånd två till tre. Dock om stationen inte lyckas associeras med nätverket så hålls det kvar på tillstånd två enda tills det lyckas med associationen. Om motförmodan en station i tillstånd två skulle få in en oautentiserad klass två ram så skickas den direkt till tillstånd ett med en *Deauthentication Frame*. Stationen får sedan börja använda sig av klass tre ramar efter att den har kommit till tillstånd tre, det är alltså vid detta tillstånd som stationen är både autentiserad och associerad. Om stationen är både autentiserad och associerad så får stationen fritt ansluta sig med andra stationer på nätverket för att överföra data (Gast, 2005). Figur 3 illustrerar ett exempel på hur dessa olika klasser används för att komma från ett tillstånd till ett annat. Se appendix A för vilka egenskaper de olika klasserna har.

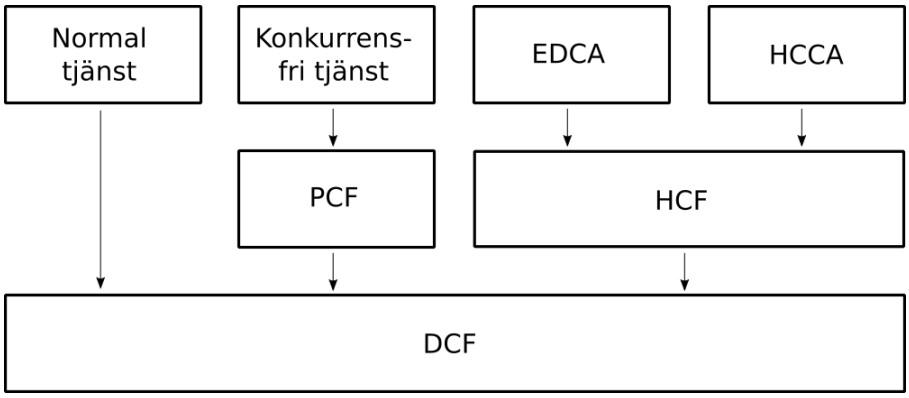
4 Koordinationsfunktioner i MAC

MAC använder sig av olika koordinationsfunktioner för att styra flödet i nätverk. Eftersom 802.11 är en trådlös teknologi så måste den visas som ett LAN för nätverkslagret. Detta LAN liknande nätverk fås med hjälp av distribuerade koordinationsfunktionen (*eng.* the distributed coordination function (DCF)). DCF är en väldigt grundläggande del av 802.11 på grund av att det är en konkurrensdriven tjänst (*eng.* contention based service). Konkurrensdriven tjänst innebär i detta fall att all trafik i nätverket levereras i samma hastighet och med samma prioritet, men att det inte garanteras att någonting kommer fram. Om det dock behövs en icke-konkurrensdriven tjänst för att styra flödet i nätverk så används



Figur 3: Exempel på hur en mobilstation ansluter sig till en AP.

punkt koordinationsfunktionen (*eng.* point coordination function (PCF)). PCF är byggt på DCF med den fördelen att PCF använder sig av en tidsbunden leverans av paket. För att garantera tjänstekvaliteten (*eng.* quality of service (QoS)) så används hybrid koordinationsfunktionen (*eng.* hybrid coordination function (HFC)) som kan tänkas vara en medelväg mellan DCF och PCF (Gast, 2005). Koordinationsfunktionerna förklaras i mera detalj i följande stycken. Figur 4 ger en överblick av koordinationsfunktionerna.

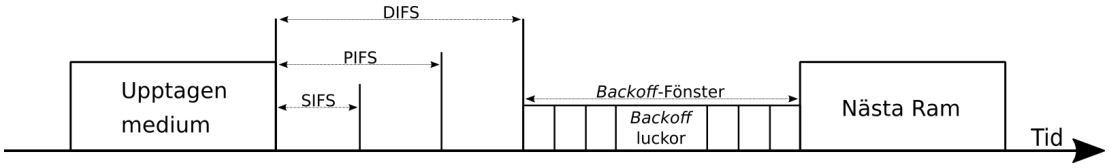


Figur 4: MAC koordinationsfunktionerna.

4.1 Åtkomstprotokoll

DCF använder sig av *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA) protokollet för att undvika kollisioner. CSMA/CA bestämmer ifall

kanaler i nätverk inte är lediga att ta emot data. Om kanalen är ledig så väntar klienten en bestämd tid tills nätverket meddelar klienten att kanalen är ledig så att klienten kan skicka data. Dessa bestämda tider kallas för *inter-frame space* (IFS). Figur 5 visar IFS tiderna gentemot varandra. Med hjälp av olika längder av IFS så kan nätverket prioritera olika sändningar mellan klienter. Korta IFS (*eng.* short IFS, SIFS) används när klienter skickar en kvittens (*eng.* acknowledgement, ACK) direkt efter att klienten har fått in ett paket. En klient som själv vill sända data över nätverket måste vänta längre och använda sig av en distribuerad IFS (*eng.* distributed IFS, DIFS) före klienten påbörjar sin sändning. Om nätverket inte är ledigt för att ta emot data så använder de sig av en så kallad *exponential backoff* algoritm för att undvika kollisioner mellan klienter. Tiden för hur länge nätverket skall vänta är i slumpmässiga intervaller beroende på *backoff* algoritmen (Gorshe m. fl., 2014). Med andra ord så kan klienten börja sändningen först efter att tiden för *backoff* algoritmen har tagit slut. DCF kan även användas sig av klar att sända/begäran om att sända (*eng.* clear to send/request to send, CTS/RTS) kollisionsundvikande tekniken för att minska risken av kollision. En av orsakerna till varför RTS/CTS används är för att undvika att klienter inom nätverket blir gömda från varandra (*eng.* the hidden terminal problem) (Holt & Huang, 2010).



Figur 5: Exempel på IFS.

The Hidden terminal problem är när klienter inom ett nätverk har åtkomst till nätverkets AP men kan inte direkt skicka och ta emot data från andra klienter. Ett scenario när detta händer är när två klienter försöker skicka data till nätverkets AP samtidigt, AP sänder sedan data vidare mellan klienterna som leder till att MAC kan inte hantera flödet ordentligt eftersom klienterna inte känner till varandra och orsakar sedan en kollision. En lösning till detta är att använda sig av CTS/RTS tekniken. CTS/RTS fungerar på det viset att klienten skickar ett RTS paket till nätverkets AP, AP skickar tillbaka ett CTS paket så att klienten tillåts skicka den data som skulle skickas från första början. På detta vis synkroniseras flödet mellan klienter för att undvika kollisioner. Lösningen skapar dock en massa latens vilket kan bli till ett större problem än själva kollisionerna.(Gorshe m. fl., 2014).

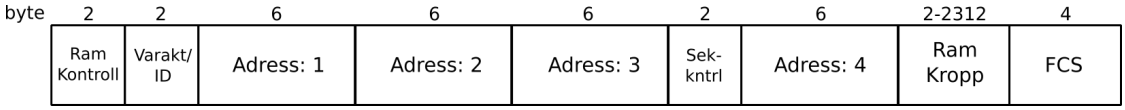
PCF är byggt rakt ovanpå DCF som man kan se i figur 4. PCF tillämpas

med punktkoordinatorer (*eng.*point coordinators) som ligger i nätverkets AP. På grund av att PCF endast kan användas med nätverk som använder sig av en AP så begränsas användningen av PCF till infrastruktur baserade nätverk. Med PCF så väntar nätverks AP på PCF interframe space (PIFS) istället för DIFS i väntan på att kanalen skall bli ledig för sändning. Eftersom PIFS har kortare tids begränsningar än DIFS så betyder det att punktkoordinatorer i PCF alltid har prioritet över kanalen den vill ha åtkomst till (Gast, 2005).

HCF som namnet säger är en hybrid mellan DCF och PCF. HCF togs med i 802.11e standarden för att ge stöd för QoS till trådlösa nätverk och som en förbättring till PCF. Med HCF kan man använda sig av två olika kanaler; enhanced distributed channel access (EDCA) och HCF controlled channel access (HCCA). EDCA medför en konkurrens driven tjänst med den skillnaden att nätverkets AP kan bestämma vilka klienter som skall ha en hög eller låg prioritet. Klienter med hög prioritet behöver naturligtvis inte vänta lika länge på att få sända data som klienter med en lägre prioritet. (Holt & Huang, 2010)

5 Formatet för MAC-dataramar

När datalänklagret får in ett meddelande från nätverkslagret för att sedan formatera meddelandet till delade dataramar så får man en så kallad MAC dataram (*eng.* MAC frame). MAC dataramen innehåller sammanlagt nio olika fält där var och en gör olika saker. Dock är vissa fält i dataramen frivilliga samt vissa fälts värden ändras beroende på vilken sorts dataram det är som man vill skicka. Figur 6 illustrerar vilka fälts som finns i en MAC dataram. Varje fält i dataramen har även en viss mängd bytes till sitt förfogande. Fälten kommer till en viss mån att gås igenom i följande stycke.



Figur 6: MAC dataram.

5.1 Ramkontroll

Varje dataram börjar med en två byte lång ramkontroll (*eng.* Frame Control) som i sin tur innehåller elva stycken underfält som visas i figur 7.

Fältet för protokollversion (*eng.* Protocol version) berättar för datalänklagret vilken sorts MAC version dataramen är av, detta görs med att tilldela en nolla eller en etta beroende på version. Än så länge så finns det endast en version av MAC så underfältet tilldelas en nolla automatiskt.

Fältet för typ och subtyp (*eng.* Type and subtype fields) indikerar vilken sorts ram det är som skickas. Det är t.ex. här som de olika koordinationsfunktionerna (DCF, PCF eller HCF) definieras att skall användas. T.ex. kunde en typ vara i still med 0100 som betyder att dataramen är tom, och ingen data således skickas. De olika subtyperna kan undersökas närmare via Gast (2005) sid 71-72.

Fältet för ToDS och FromDS berättar för datalänklagret om dataramen är påväg till ett distribuerat system eller inte. T.ex. om biten i ToDS är 0 och biten i FromDS 1 så tolkas det som att dataramen skickas till en trådlös station i ett infrastrukturbaserat nätverk.

More fragments bit fältet indikerar om dataramen har blivit fragmenterad. Fältet sätts till en etta om det är fragmenterat och en nolla om inte.

Försök igen (*eng.* Retry) fältet sätts till en etta om dataramen skall sändas på nytt, en nolla om inte.

Fältet för energihantering (*eng.* Power management) indikerar om den sändande enheten är i energisparläge. Etta om den är det och en nolla om inte.

Om en enhet är i energisparläge så sätts fältet för mera data (*eng.* More data) till en etta för att indikera att nätverkets AP har en eller flera dataramar som är för enheter i sömn/energisparläge läge. På detta vis så vet nätverkets AP lägga en buffert på data som skall skickas till de sovande enheterna.

Fältet för skyddad ram (*eng.*Protected frame) indikerar om dataramen är skyddad av datalänklagrets säkerhets protokoll. En etta indikerar om dataramen är skyddad och en nolla berättar om den inte är.

Fältet för ordning (*eng.* Order) indikerar med en etta om dataramen och dess fragment skall skickas i ordning och en nolla om inte. (Gast, 2005) (Holt & Huang, 2010)

Figur 7: Fältet för ramkontroll.

5.2 Varaktighet/ID

Fältet för Varaktighet/ID (*eng.* Duration/ID) är upplagt av 16 bitar (0-15) och anger mängden tid som kan användas för att sända och ta emot en ACK. Detta görs med att ange läget på närliggande enheternas *Network Allocation Vector* (NAV). T.ex. om sista den biten i fältet är lagd till 0 (bit 15) så representerar bitarna 0-14 tiden för hur länge mediet skall vänta tills den får börja sända. Mera detaljerad information om *Duration/ID* finns att läsa från (Gast, 2005).

5.3 MAC-adress

En MAC-adress är en 48-bit lång unik identifierare av nätverkskort (*eng.* network interface controller (NIC)) i diverse enheter som t.ex. bärbara datorer eller bordsdatorer. Adressen består av sex stycken oktetter varav varje oktett består av åtta bitar. Bitarna i varje oktett kan antingen vara en nolla eller en etta som gör att det finns 2^{48} olika MAC-adresser. Strukturen på adressen visas i figur 8. Användingen av MAC-adresser är inte begränsat till endast 802.11 teknologier utan används också av andra teknologier som 802.3 (LAN datornätverk) och Bluetooth. Som sagt så är MAC-adressen en del av MAC protokollet som i sig själv är ett underlager till datalänklagret (Martin m. fl., 2017).

MAC-adresser tilldelas oftast i block av olika storlekar som enhetstillverkare kan köpa från IEEE. Det vanligaste blocket som företag införskaffar är MAC Address Block Large (MA-L) eller Organizationally Unique Identifier (OUI) som visas i figur 8. OUI blocken består av tre stycken oktetter som registreras till tillverkare som sedan tar över kontrollen av MAC-adresserna för att användas i sina respektive enheter. Efter att OUI blocket har registrerats så måste företaget själv definiera de tre sista oktetterna i adressen, dvs de definierar NIC-blocket som endast används internt hos tillverkaren och måste vara unik.

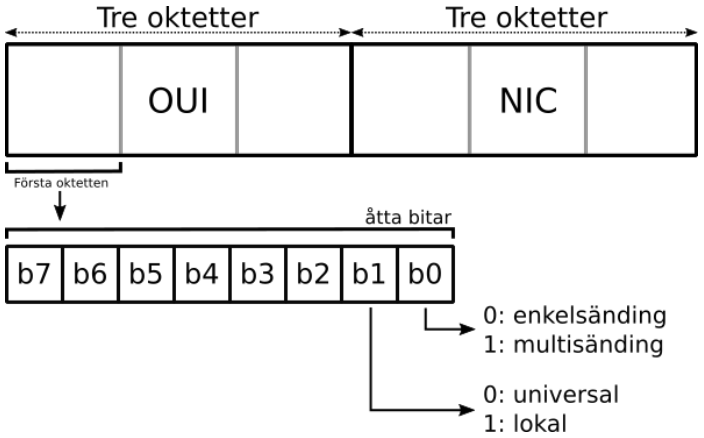
Med tanke på att OUI är en för allmänheten unik identifierare så är det rätt så enkelt att lista ut vem tillverkaren är på en enhet med hjälp av att kolla på MAC-adressen. För att undvika detta så har tillverkare möjligheten att köpa privata OUI block av IEEE. Dessa privata block döljer tillverkarens namn i registret som gör det svårare att identifiera enhetens ursprung. Dock har det visats av Martin m. fl. (2017) att det är ovanligt för tillverkare att använda sig av denna tjänst.

MAC-adresser kan antingen vara universala (*eng.* universally administered adresses) eller lokala (*eng.* locally administered adresses) beroende på första oktettens näst sista bit. En nolla tyder på att adressen är universal medan en etta

lokal. Universala adresser tilldelas av tillverkare unikt för enheter. Lokala adresser tilldelas av nätverksadministratorer för att överskriva den universala adressen. Ett exempel på användningen av lokala adresser skulle vara med anslutningspunkter, service set identifiers (SSID) som är en id-nummer för att åtskilja trådlösa nätverk från varandra. Med hjälp av lokala adresser så kan enheter ta nytta av MAC-adress randomisering för att skapa slumpmässiga MAC-adresser (Martin m. fl., 2017). MAC-adress randomisering tas upp i mera detalj i följande kapitel.

Näst sista biten i den första oktetten definierar om MAC-adressen är för enkelsändning (*eng.* unicast) eller multisändning (*eng.* multicast). Enkelsändning innebär att adressen representerar en station gentemot multisändning som representerar en grupp av stationer. (Gast, 2005)

Som figur 6 hänvisar till så finns det fyra olika adress fält som kan användas bereonde på dataramens typ. Typen av adress definieras av fältet för ToDS och FromDS som förklarades i kapitel 5.1 om ramkontroll. För en mera detaljerad förklaring om hur ToDS och FromDS fungerar så hänvisas läsaren till Holt & Huang (2010) sid 39. Vanligen så används den första adressen som mottagare, andra adressen som sändare och den tredje adressen för filtrering av sändaren medan den fjärde adressen lämnas tom. (Holt & Huang, 2010)



Figur 8: Strukturen på en MAC-adress.

5.4 MAC-adress randomisering

MAC-adress randomisering (*eng.* MAC-address randomization) är en teknik som slumpmässigt växlar genom unika hårdvaruadresser för att göra det svårare för aktörer att lyssna in på datatrafik som t.ex. skulle vilja lokalisera enskilda enheter ur mängden. Dessvärre har denna teknik haft en ganska oregelbunden tillämpning

från tillverkare. Tillämpningen i sig själv har heller ingen fastställd standard utan alla tillverkare har sitt ägna sätt för att utföra randomiseringen. Tillämpningen är inte bara annorlunda på operativsystemets (OS) nivå utan kan skilja sig från en enhet till en annan. Det finns även vissa brister i hur tillverkare använder sig av tekniken som lätt kan kringgås, som visas av Martin m. fl. (2017). Denna avhandling kommer endast att gå i detalj igenom randomiseringen för mobiltelefoner med Android och iOS OS fast tekniken även kan användas för andra OS som Windows och Linux.

5.4.1 Android randomisering

Första Android versionen som använde sig av MAC-adress randomisering var Android 6.0 med så kallade sondförfrågningar (*eng.* Probe request) (Vanhoef m. fl., 2016). I Android 8.0 uppdaterades tekniken till att randomisera adressen medan enheter söker efter nya nätverk. Randomiseringen händer alltså inte om enheten redan är associerad med nätverket från tidigare. Android 9 gav möjligheten att randomisera adressen före anslutning oavsett om enheten tidigare varit ansluten till nätverket eller inte, dock var detta avstängt som standard. (Google, 2020)

En sak som också är värd att nämna är att alla tillverkare av Android mobiltelefoner har sina egna versioner av randomisering, det finns alltså ingen fastlagd standard som alla använder.

5.4.2 iOS randomisering

Första iOS versionen som använde sig av MAC-adress randomisering var Apple iOS 8. Randomiseringen händer i princip endast om enheten inte är associerad med nätverket eller om enheten är i sov läge. iOS 9 uppdaterade ytterligare tekniken till att även randomisera adressen medan enheten är i användning (Vanhoef m. fl., 2016).

Apple använder naturligtvis samma teknik på alla enheter för att randomisera eftersom de är den enda tillverkaren av iOS mobiltelefoner.

6 Metoder för att missbruka 802.11 säkerhet

Dessa metoder eller attacker som man också kan kalla dem används i första hand för att införa en så kallad person-i-mitten-attack (*eng.* Person-In-The-Middle, PITM). PITM attacker är som namnet säger, en tredje part som försöker avläsa meddelanden som skickas mellan klienten och nätverkets AP. I de flesta fallen så tror klienten och AP att de kommunicerar direkt med varandra, men i själva verket så går kommunikationen rakt till den tredje parten som i värsta fall kan manipulera meddelandena. Ett exempel på en manipulation kunde vara att tredje parten använder sig av en bluffsida för att vidare kunna extrahera privat information av klienten. Ofta använder denna tredje part också en falsk AP (*eng.* Rogue Access Point) för att effektivt lura klienter att ansluta till sitt nätverk.

Orsaken till att detta är möjligt är för att 802.11 standarden inte specificerar på vilket sätt klienter skall ansluta sig till nätverk. Standarden låter också klienter att ansluta sig fritt mellan AP (med samma SSID) inom nätverket för att förhindra att klienten tappar anslutningen om klienten flyttar på sig (*eng.* Roaming). Standarden hänvisar inte heller till hur klienten skall bestämma sig för vilken AP som skall anslutas till.

Det är också värt att nämna att dessa attacker kan kombineras med andra metoder för att öka chansen att av att klienter ansluter sig till falska AP. Exempel på dessa metoder kunde vara att skicka deautentiserings ramar till den riktiga AP, i princip är detta som att göra en *Denial-of-Service* (DoS) attack på en webbsida. Medan den riktiga AP störs så kan den falska AP förstärka sin signal och på sätt se ut som den riktiga AP, vilken i sin tur får klienter att ansluta sig till den falska AP istället. Solstice.sh (u. å.); Ryan (2019a)

6.1 Nätverksval

Avhandlingen kommer att ta upp två olika sätt som klienter använder sig av för att välja vilket nätverk de vill ansluta sig till, nämligen passiv skanning och aktiv skanning.

6.1.1 Passiv Skanning

Passiv skanning sker när ett nätverk skickar ut *Beacon Frames* med jämna mellanrum (Oftast varje 100ms) för att annonsera för alla närliggande klienter att detta nätverk finns och det går att anslutas till. Dessa *Beacon Frames* har med sig information om hurudant nätverk det handlar om, hurudana hastigheter nätverket stöder, om det är krypterar, m.m. Dock den viktigaste informationen som ramen för med sig är nätverkets SSID.

Klienter som lyssnar och tar emot dessa *Beacon Frames* kollar om de tidigare har anslutit sig till ett nätverk med samma SSID. Om klienten känner igen nätverkets SSID så ansluter klienten sig till nätverket automatiskt. (Dai Zovi & Macaulay, 2005)

6.1.2 Aktiv Skanning

Aktiv skanning eller aktiv avsökning (*eng.* Active Probing) som det även kallas sker när klienter aktivt skickar ut sondförfrågningar för att avgöra om och vilka nätverk som är i närheten, på samma gång så skickar även nätverk information om sig själv till klienten.

Dessa sondförfrågningar kan användas på två olika sätt, riktad sändning och bred utsänding (*eng.* Broadcast). Riktade sondförfrågningar skickas endast till nätverk som klienten tidigare har varit ansluten till, med andra ord till specifika SSID. Klienten gör detta kontinuerligt för alla SSID som den känner till och slutar endast om den ansluts något av dessa nätverk. Bred utsända sondförfrågningar skickas istället till alla nätverk i närheten utan att först kolla om nätverken har anslutits till tidigare. På detta vis så kan klienten kolla om tidigare anslutna nätverk finns i närheten utan att avslöja för andra vilka dessa tidigare nätverk är. (Dai Zovi & Macaulay, 2005)

6.2 Evil Twin

På grund av att 802.11 standarden inte kräver att anslutningspunkter skall autentisera sig för klienter så kan Evil Twin attacker missbruka processen för att lura klienterna att ansluta sig till sin falska AP. Som det förklarades i kapitel 3.3 så krävs det att AP skall autentisera sig först efter att klienten har skickat en *Beacon Frame* för att meddela att klienten är redo att ansluta sig till nätverket. Evil Twin attacker fungerar med att skapa en falsk AP med samma SSID som klienten tidigare har anslutit sig till och kan på detta vis tvinga klienten att ansluta sig till den falska AP. Evil Twin skickar alltså ut en *Beacon Frames* med samma information (specifikt samma SSID) som den riktiga AP för att lura klienten att tro att den falska AP är den riktiga. Nackdelen med denna attack är att den som utför attacken måste veta från tidigare vilka nätverk som klienten tänker ansluta sig till.

På samma sätt så kan Evil Twin attacker missbruka *Roaming* funktionaliteten hos mobila klienter. Detta kan göras på två olika sätt, första sättet är att locka klienten med en bättre signal på den falska AP jämfört med den riktiga AP. Andra sättet är att blockera tillgången till den riktiga AP med t.ex. en DoS attack, vilket naturligt får klienten att ansluta sig till den falska AP istället. (Solstice.sh, u. å.; rootsh3ll, u. å.)

Evil Twin attacker missbrukar säkerheten i passiv skanning som orsakas av att 802.11 standarden inte kräver att AP skall autentisera sig för klienter. Som det förklarades i kapitel 3.3 om uppkopplingsekvenser så autentiseras klienten endast när den har bestämt sig för att ansluta till ett nätverk. Evil Twin attacker fungerar med att skapa en falsk AP med samma SSID som klienten tidigare har anslutit sig till. På detta vis så tvingas klienten att ansluta sig den falska AP eftersom den falska AP skickar ut *Beacon Frames* med samma information (specifikt samma SSID) som den riktiga AP.

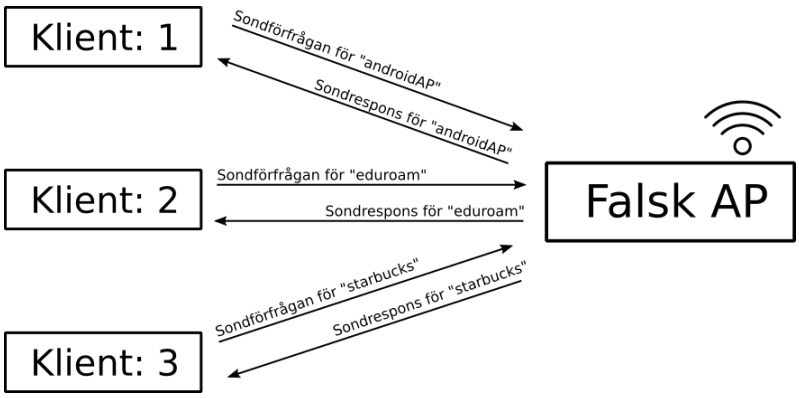
6.3 Karma

Karma attacker tar nytta av klienter som använder sig av aktiv skanning. Som sagt så skickar nätverk periodiskt ut *Beacon Frames* med jämna mellanrum. Enligt 802.11 standarden så skall dessa nätverk endast svara på sondförfrågningar från klienter som är rakt riktade mot nätverket. Med Karma attacker så modifierar man dock nätverken att svara på alla sondförfrågningar i närheten. Som det illustreras i figur 9 så tar falska AP emot alla sondförfrågningar och således skickar tillbaka

sondresponser från klienter, vilket i sin tur leder klienterna till att ansluta sig till nätverket som de tror är det riktiga nätverket.

Till skillnad från Evil Twin attacker så behöver inte Karma attacker vara i närheten av den riktiga AP. Falska AP som använder sig av Karma så skickar inte heller ut signaler till klienter för att meddela att det är ett nätverk som de kan ansluta sig till. Med andra ord så svarar endast den falska AP på sondförfrågningar som den väljer att ta emot.

Man skulle kanske kunna tro att gömda nätverk är immuna till attacker som dessa. Med tanke på att Karma attacker utnyttjar sondförfrågningar från klienter i närheten, så påverkas även dessa nätverk eftersom klienter som tidigare har varit anslutna till nätverken även måste skicka ut förfrågningar för att hitta och ansluta sig till dem. (Dormann, 2015; Chatzisofroniou, 2018)



Figur 9: Exempel på hur Karma attacken fungerar.

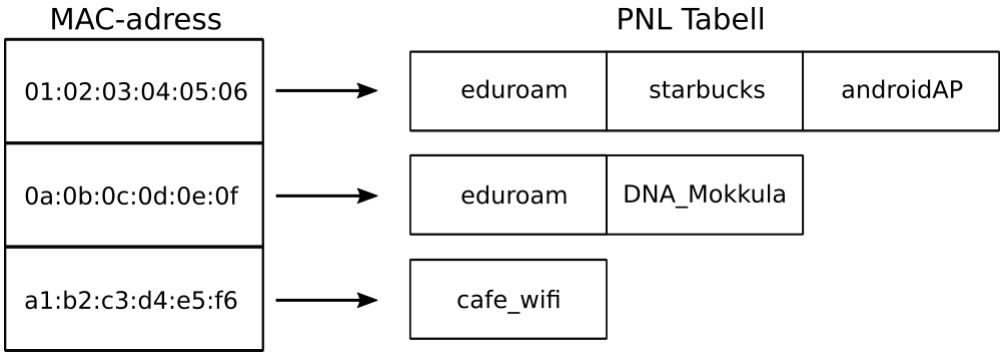
6.3.1 MANA

MANA står för *MITM And Network Attack* och gör precis som namnet säger, använder sig av en nätverksattack för att implementera en MITM attack (Avhandligen använder sig av PITM som betyder samma sak som MITM). MANA attacker är en förbättring på Karma attacken med att istället för att den tredje parten måste gissa sig till eller veta från tidigare till vilka nätverk som klienten har anslutit sig till så kan MANA återskapa nätverks föredragna nätverkslistor (*eng.* Preferred Network Lists) (PNL). PNL är i princip det som nämnts tidigare om hur klienter automatiskt ansluter sig till nätverk, det handlar alltså om en lista av information om nätverk som klienten tidigare har anslutit sig till.

Som nämndes i kapitel 6.3 så svarar Karma attacker på slumpmässiga sondförfrågningar vilket inte lär fungera mera på de flesta moderna enheterna. Pro-

blemet är att dessa enheter fullständigt ignorerar sondförfrågningar från nätverk som inte först har skickat ut en *Broadcast Probe* som nämndes i kapitel 3.3 om uppkopplingssekvenser.

MANA attacker kringgår detta problem med att ta up och lagra MAC-adresserna från klienter i en hashtabell. MAC-adresserna kommer från sondförfrågningarna som falska AP får in från klienterna. Varje MAC-adress i hastabellen har i sin tur information om vilka SSID som klienten har skicka ut sondförfrågningar till. På detta vis så rekonstruerar MANA attacken närliggande klienters PNL. Figur 10 ger ett exempel på hur en hashtabell ser ut i MANA.



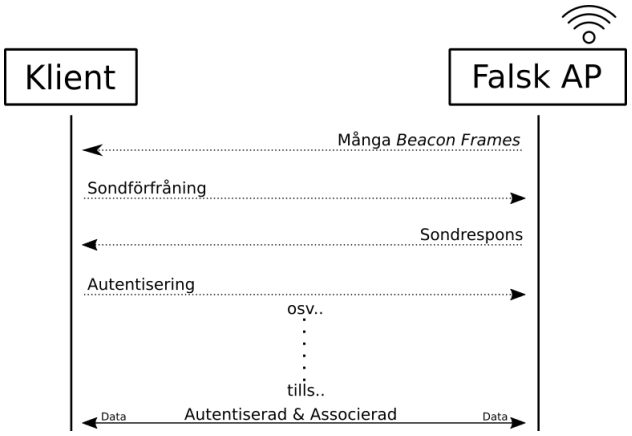
Figur 10: Exempel på en hash tabell som används i MANA attacker.

En annan variation av MANA attacker är Loud Mode. Till skillnad från MANA attacker som skickar ut en sondförfrågan för varje SSID i klientens PNL så skickar Loud Mode ut sondresponser för varje SSID i varje PNL för varje klient som den falska AP har utbytt information med. Med Loud Mode attacker så kan man alltså även komma åt klienter som borde vara säkra från vanliga Karma/MANA attacker med att utnyttja den dåliga säkerheten av en annan klient i närheten. (Ryan, 2019b)

6.4 Known Beacons

Known Beacons attacker används på enheter som är immuna för Karma/MANA attacker. Known Beacons i sin enkelhet använder sig av en lista av vanligt använda SSID som t.ex. AndroidAP eller DNA-Mokkula som används för att skicka ut *Beacon Frames* till. Det handlar alltså endast om nätverk som vanligtvis används och är öppna, inte direkt riktade nätverk som tidigare attacker har använts för. För att maximera åtkomsten av klienter så kan tredje parten även använda sig av en Karma/MANA attack på samma gång.

Known Beacons är en av attackerna som utnyttjar enheters användning av automatisk anslutning för att lura dem att anslutas till falska AP. (Chatzisofroniou, 2018) Figur 11 illustrerar hur Known Beacons attacken fungerar i praktiken.



Figur 11: Diagram på hur Known Beacons attacken fungerar.

6.5 Timing Attacker

Timing attacker är ett exempel på en attack som kan kringgå säkerheten med MAC-randomisering. Hur randomiseringen kringgås är att skicka ut en grupp av sondförfrågningar med jämna mellanrum (typiskt mindre än 500ms) och sedan meta tiden som går mellan själva förfrågningarna men också mellan grupperna. Mellan rummet mellan dessa förfrågningar kallas för *Inter-Frame Arrival Time* (IFAT). Med hjälp av en kombinationen av tiden som mättes mellan grupperna och de enskilda förfrågningar i grupperna så kan man skapa ett unikt ”fingeravtryck” av enheten man försöker komma åt. På detta vis så kan man spåra enheter oberoende om enheten är i användning av randomisering eller inte (Matte m. fl., 2016). Matte m. fl. (2016) förklarar algoritmen bakom Timing attacker i mera detalj i sin artikel.

7 Sammanfattning

WiFi nätverk är i stor användning runt om i världen och kan vara väldigt känsliga för intrång, speciellt om nätverken är öppna för allmänheten som i ett café. Intrången kan motiveras av att en tredje part vill t.ex. ha tillgång till personers privata information, som t.ex. nätverkstrafik, MAC-adresser eller helt enkelt bara för att spåra enheten som personen använder. Ofta är dessa attacker av skadlig avsikt, men kan även användas för så kallade penetrationstester som har som avsikt att hitta fel i nätverkssäkerheten för att förbättra den. Dock kommer avhandlingen inte gå något närmare in i varför och hur man kan använda sig av dessa attacker. Däremot vill skribenten nämna några tips om hur man kan vara säkrare när det gäller att försäkra sig mot dessa attacker och varför man egentligen inte behöver oroa sig något desto mera om dem.

Det första tipsen kommer att vara ganska självklart för majoriteten av läsarna, men försök att undvika användningen av öppna nätverk så mycket som möjligt. Det är som sagt vid öppna nätverk som de flesta av dessa attacker tas i bruk. Det är också värt att nämna att andra användare av nätverk kan lätt övervaka trafiken med paketanalysator program, där de kan få fram information om andra användare på nätverk (beroende på hur säkert nätverket är). Om användaren redan från tidigare har anslutit sig till något öppet nätverk så är det rekommenderat att direkt ta bort informationen om dessa nätverk från sin enhet eftersom de kan fortfarande utnyttjas i attacker som Karma och MANA. Vissa operativ har även funktionalitet för att begränsa enheters association (se kapitel 3.3 om mera information) till nätverk som enheten har meddelat sin MAC-adress till. På det viset så undviker man till exempel attacker som Karma (se kapitel 6.3 om mera information). Nätverk som använder sig av gömda SSID är inte så säkra som man skulle tro, tvärt emot så kan de vara ännu mer sårbara för vissa attacker. Speciellt attacker som använder sig av sondförfrågningar och sondresponser för att missbruka säkerheten hos klienter. Klienter måste nämligen skicka ut sondförfrågningar till nätverken för att hitta dem, som i sin tur uppger för tredje parter vilket nätverk det är som klienten vill ansluta sig till. Ett enkelt sätt att undvika attackerna som nämnts i kapitel 6 är att helt enkelt stänga av WiFi när det inte är i användning. Anslut sedan manuellt till nätverken istället för att använda sig av automatisk anslutning som redan har nämnts att är sårbart för attacker.

Referenser

Akyildiz, I. F. & Xudong Wang. (2005, Sep.). A survey on wireless mesh networks. *IEEE Communications Magazine*, *43*(9), S23-S30. doi: 10.1109/MCOM.2005.1509968

Alliance, W. (u. å.-a). *Wi-Fi Alliance who we are.* Hämtad 2020-02-06, från `https://www.wi-fi.org/who-we-are`

Alliance, W. (u. å.-b). *Wi-Fi Alliance wi-fi certified ac.* Hämtad 2020-02-22, från `https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-ac`

Chatzisofroniou, G. (2018). *The known beacons attack (34th chaos communication congress).* Census. Hämtad 2020-03-19, från `https://census-labs.com/news/2018/02/01/known-beacons-attack-34c3/`

Dai Zovi, D. A. & Macaulay, S. A. (2005, June). Attacking automatic wireless network selection. I *Proceedings from the sixth annual ieee smc information assurance workshop* (s. 365-372). doi: 10.1109/IAW.2005.1495975

Dignited. (u. å.). *Dignited the difference between wi-fi and lte.* Hämtad 2020-02-07, från `https://www.dignited.com/34634/the-difference-between-wi-fi-and-lte/`

Dormann, W. (2015). *Instant karma might still get you.* Carneie Mellon University. Hämtad 2020-03-19, från `https://insights.sei.cmu.edu/cert/2015/08/instant-karma-might-still-get-you.h`

Electronics Notes. (u. å.). *Electronics Notes what is ofdm: Orthogonal frequency division multiplexing.* Hämtad 2020-02-20, från `https://www.electronics-notes.com/articles/radio/multicarrier-modulation/ofdm`

Faircloth, J. (2014). Chapter 2 - networks. I J. Faircloth (red.), *Enterprise applications administration* (s. 27 - 79). Boston: Morgan Kaufmann. Hämtad från `http://www.sciencedirect.com/science/article/pii/B9780124077737000028` doi: https://doi.org/10.1016/B978-0-12-407773-7.00002-8

Gast, M. S. (2005). *802.11 wireless networks: The definitive guide, second edition.* O'Reilly Media, Inc.

Gast, M. S. (2013). *802.11ac: A survival guide* (1st utgåvan). O'Reilly Media, Inc.

Google, A. (2020). *Privacy: Mac randomization.* Hämtad 2020-03-12, från https://source.android.com/devices/tech/connect/wifi-mac-randomization

Gorshe, S., Raghavan, A., Starr, T. & Galli, S. (2014). *Broadband access: Wireline and wireless - alternatives for internet services.* doi: 10.1002/9781118878774

Holt, A. & Huang, C.-Y. (2010). *802.11 wireless networks security and analysis.* doi: 10.1007/978-1-84996-275-9

Intel Corporation. (2019). *Intel Corporation learn about multiple-input multiple-output.* Hämtad 2020-02-20, från https://www.intel.com/content/www/us/en/support/articles/000005714/network-an

Lammle, T. (2009). *Comptia network+ deluxe study guide: Exam n10-004.* Wiley. Hämtad från https://books.google.fi/books?id=5QRnPPfpuMgC

Martin, J., Mayberry, T., Donahue, C., Foppe, L., Brown, L., Riggins, C., ... Brown, D. (2017). A study of MAC address randomization in mobile devices and when it fails. *CoRR*, *abs/1703.02874*. Hämtad från http://arxiv.org/abs/1703.02874

Matte, C., Cunche, M., Rousseau, F. & Vanhoef, M. (2016, 07). Defeating mac address randomization through timing attacks. I (s. 15-20). doi: 10.1145/2939918.2939930

rootsh3ll. (u. å.). *Evil twin attack: The definitive guide.* Hämtad 2020-03-19, från https://rootsh3ll.com/evil-twin-attack/

Ryan, G. (2019a). *Modern wireless tradecraft pt i — basic rogue ap theory — evil twin and karma attacks.* Specterops. Hämtad 2020-03-19, från https://posts.specterops.io/modern-wireless-attacks-pt-i-basic-rogue-ap-theor

Ryan, G. (2019b). *Modern wireless tradecraft pt ii — mana and known beacon attacks.* Specterops. Hämtad 2020-03-22, från https://posts.specterops.io/modern-wireless-attacks-pt-ii-mana-and-known-beac

SecureEdge. (2016). *SecureEdge what's the difference between 802.11ac wave 1 and wave 2?* Hämtad 2020-02-22, från https://www.securedgenetworks.com/blog/whats-the-difference-between-802.11ac-

Solstice.sh. (u. å.). *Attacking and gaining entry to wpa2-eap wireless networks.* Hämtad 2020-03-22, från http://solstice.sh/workshops/advanced-wireless-attacks/ii-attacking-and-gaini

Suri, P. R. & Rani, S. (2007, March). Bluetooth network-the adhoc network concept. I *Proceedings 2007 ieee southeastcon* (s. 720-720). doi: 10.1109/SECON.2007.342994

Vanhoef, M., Matte, C., Cunche, M., Cardoso, L. S. & Piessens, F. (2016). Why mac address randomization is not enough: An analysis of wi-fi network discovery mechanisms. I *Proceedings of the 11th acm on asia conference on computer and communications security* (s. 413–424). New York, NY, USA: Association for Computing Machinery. Hämtad från https://doi.org/10.1145/2897845.2897883 doi: 10.1145/2897845.2897883

Wikipedia. (2015). *Offnfopt: Osi-modellen - eget arbete.* Hämtad 2020-02-10, från https://commons.wikimedia.org/w/index.php?curid=39917431

Appendix A

Tabell över uppkopplingssekvenserna i 802.11

Klass ett		
Kontroll	Hantering	Data
RTS CTS ACK CF-End CF-End+CF-Ack	Probe Request Probe Response Beacon Authentication Deauthentication Announcement Traffic Indication Message (ATIM)	Vilken ram som helst som har ToDS och FromDS satt till 0.

Klass två		
Kontroll	Hantering	Data
Ingen	Association Request/Response Reassociation Request/Response Disassociation	Ingen

Klass tre		
Kontroll	Hantering	Data
Ingen	Deauthentication	Vilken ram som helst ingen skillnad vad ToDS och FromDS är satta till.

Tabell 2: Klass ett två och tre med deras egenskaper. (Gast, 2005)