1. Sammendrag

Vi har gjennom denne teksten sett på forskjellige sikkerhetsaspekter ved 802.11, som er en trådløs standard for lokalnettverk. 802.11 operer innenfor 2.4GHz og 5GHz, der 2.4GHz er det som er klart mest brukt av disse to. Disse områdene er fritt brukbare for alle, og når 2,4GHz kun har 3(4) kanaler som ikke overlapper, begynner disse områdene å bli ganske fulle i tett befolkede områder. Dette vil føre til sterkt redusert ytelse, og være en seriøs hindring for tilgjengeligheten.

802.11 har svakheter i forbindelse med metoder på MAC-laget som fører til at det er mulig å kjøre en rekke DoS (Denial of Service) angrep på basestasjonen. Eksempel på slike angrep er deauthentication angrep og deassosiation angrep. Disse angrepene krever lite hardwareressurser, og er svært fleksible. Man kan stenge ute en enkelt klient om man vil. Arbeid for å forebygge disse svakhetene er påbegynt, men er enda ikke ferdig, slik at dette fremdeles er en stor sikkerhetsrisiko som er lett for angripere å utnytte. Før disse er fikset, kan de være en stor risiko for folk som er avhengig av tilgang til enhver tid.

I starten hadde 802.11 lite sikkerhetstiltak. Det fantes få og dårlige løsninger for å sikre aksesskontroll. Blant disse er skjult SSID og MAC-filtrering. Begge disse er dog lette å omgå.
WEP (Wired Equivalent Privacy), som var den første metoden for å sikre konfidensialitet, og som også samtidig tilbød litt autentisering. Når WEP i 2001 derimot ikke viste seg å være en for god sikkerhetsmekanisme og ble knukket, var det ingen direkte arvtaker til denne. 802.11i var under arbeid, men ble ikke ferdig før i 2004. Dette førte til at en Wi-Fi Alliance innførte en midlertidig metode for å sikre konfidensialitet, integritet og autentisitet. Metoden ble kalt WPA (Wi-Fi Protected Access). WPA bruker samme chiffer som WEP, men innfører TKIP (Temporal Key Integrity Protocol) som fjerner svakhetene ved WEP.

802.1x var en annen teknologi som ble innført ved WPA. 802.1x er en autentiseringsløsning som allerede var utviklet for Ethernet, men ble nå også integrert med 802.11. 802.1x gir dermed 802.11 en god autentiseringsmetode, som også gir oss gjensidig autentisering. 802.1x er avhengig av endel infrastruktur, blant annet en autentiseringstjener, noe som gjør dette litt mer krevende å installere. Det kan dog lett kobles opp til å bruke autentiseringsinformasjon for brukere i allerede eksisterende løsninger. For nettverk som ikke ønsker så mye infrastruktur kan man bruke WPA med en såkalt pre-shared key. Dette er en nøkkel som manuelt tastes inn på alle deltakere i det trådløse nettverket.

I 2004 ble 802.11i standardisert. Siden et av målene med WPA var å sikre forover og bakover kompabilitet, tilførte ikke denne standarden mye nytt, utenom en ny chiffer AES (, som er enda sikrere enn TKIP. 802.11i kom også med 802.1x og TKIP. Pga disse likhetene fikk også 802.11i navnet WPA2. Det har i den siste tiden blitt begynt å dukke opp svakheter i TKIP, og man anbefaler derfor å bruke AES.

2. Innledning

2.1 WLAN - 802.11

WLAN (Wireless Local Area Network) er en teknologi som tilbyr lokale trådløse nettverk. Den mest utbredte WLAN-løsningen i verden idag er IEEE 802.11, også ofte kalt Wi-Fi. Andre utbredte WLAN-teknologier har veldig liten utbredelse, og pga av dette vil kun IEEE 802.11 diskuteres utgangspunkt.

Bruken av 802.11 har tatt svært av de siste årene. Bredbånd, og dermed konstant oppkobling mot internett har blitt allemannseie. Det samme har også bærbare datamaskiner. Med dette følger også ønsket om å kunne være på internett uten å være avhengig av å være tilkoblet et punkt i veggen. Mange bredbåndsleverandører leverer nå ut rutere med innebygd 802.11 støtte, slik at kundene automatisk får trådløst bredbånd i hjemmet. Det er også vanlig for bredbåndsleverandører/telefonileverandører å levere «Hotspots», og mange kafeer, flyplasser o.l. tilbyr trådløse soner hvor de besøkende kan gå på internett, enten gratis eller mot betaling. Mange bedrifter har også trådløse nettverk. Dette gjør det lettere for brukere med bærbare datamaskiner å forflytte seg rundt i lokalene.

WLAN kan brukes i forskjellige oppsett. Den vanligste metoden er å ha en infrastruktur. En node i nettverket får da ansvaret for å holde orden på all trafikken. Denne noden kaller vi et aksesspunkt. All trafikk vil gå gjennom dette aksesspunkt. En av de andre metodene er å ha et ad-hoc nettverk. Her kommuniserer alle datamaskinene direkte med hverandre, uten noen form for infrastruktur. Denne teksten vil kun adresse 802.11 nettverk med infrastruktur.

2.2 Problemstilling
På hvilke måter sikrer 802.11 sikkerhet? Hvilke sikkerhetshull finnes i 802.11, og hvilke tiltak er gjort/gjøres for å bedre disse svakhetene?

2.3 Avgrensning av oppgaven
Jeg vil ikke prøve å ta tak i alle sikkerhetsfeil, men å finne de viktigste og mest kritiske. Jeg vil heller ikke gå for mye detaljer på alle sikkerhetsproblemene. I tillegg vil den historiske utviklingen bli lagt litt vekt på

2.4 Oppbygging av oppgaven
Del 3 omhandler teknisk informasjon rundt 802.11.
I del 4 (tilgjengelighet) diskuteres det først hvordan frekvensressurser, antall brukere, og annet utstyr påvirker tilgjengeligheten til 802.11. Deretter ser vi litt på hvilke angrep som kan føre til at tilgjengeligheten blir mistet, hvordan disse utnyttes, og hvilke prosesser som er igang for å forbedre disse.
I del 5 ser vi på hvilke mekanismer som finnes i 802.11 med tanke på autentisering og aksesskontroll.
Vi flytter så fokuset til konfidensialitet og integritet i del 6. Vi studerer her mekanismer i 802.11 for å forbedre sikkerheten på disse områdene. Denne delen inneholder noe informasjon som også kunne ha blitt plasser i del 5, men som har funksjonalitet innenfor begge områder
Til slutt konkluderer vi i del 7.

3. WLAN - IEEE802.11
802.11, også kjent som WiFi, er en familie av standard som ble innført av IEEE i 1999. Denne standarden spesifiserer trådløs kommunikasjon for lokale nettverk. Arbeidet med tillegg til 802.11 foregår fremdeles, og legges til standarden underveis. Disse tilleggene får ofte navn hvor 802.11 etterfølges av 1-2 bokstaver. Et av de siste eksemplene på dette er 802.11n, som gikk fra å være et utkast til å bli sertifisert i oktober 2009.

Den første 802.11 standarden baserte seg på DSSS (Direct Sequence Spread Spectrum) modulering, hadde en makshastighet på 2MBit/s og en maksavstand på 20m.
I 1999 kom de første tilleggene som ga bedre hastigheter og muligheter for lengre avtander. Disse nye tilleggene var 802.11a og 802.11b. 802.11a ga oss makshastigheter på 54MBit/s med en maksavstand 35 meter ved å bruke OFDM modulasjon. 802.11a jobber på 5GHz. 802.11b ga oss makshastigher på 11MBit/s med samme maksrekkevidde som 802.11a.

Den mest brukte 802.11 standarden er 802.11g, som kom i 2003. 802.11g angir en radioforbindelse med OFDM (Orthogonal Frequency Division Multiplexing) eller DSSS modulasjon på 2,4GHz med maks teoretisk hastighet på 54Mbit/s.

Selv om 802.11n ikke ble standardisert før i oktober 2009, var det mange leverandører som hadde begynt å implementere denne standarden før det. Siden dette tillegget er relativt nytt, er det mange som ikke har utstyr som bruker dette enda. Man vil nok se en forandring i dette etter hvert som folk oppdaterer utstyret sitt.
802.11n bruker OFDM modulasjon på 2,4GHz og 5GHz, og maks teoretisk hastighet er 150Mbit/s. 802.11n støtter også muligheten for MIMO (multiple-in multiple-out), som bruker flere kanaler samtidig for å få en større datarate.
For å komme opp i 150Mbit/s må 802.11n bruke 2 kanaler med båndbredde 20 MHz. I 802.11g er kun en kanal på 20MHz brukt. Dersom 802.11n kun skal bruke en kanal, blir makshastighet 72,2 MBit/s.

802.11 er kompatibel med Ethernet standarden, og bruker et MAC-lag som ligger over det fysiske laget, og er kompatibel med Ethernet. Det er derfor enkelt å lage 802.11 utstyr som snakker med vanlige lokale nettverk.

802.11 var i utgangspunktet designet med lite fokus på sikkerhet. I mai 2003 ble et arbeid med 802.11i påbegynt. Målet med 802.11i var å utbedre sikkerheten til 802.11. 802.11i ble standardisert i juni 2004.

4. Tilgjengelighet

2.4GHz - Fritt tilgjengelig

802.11 opererer som sagt i frekvensområdene 2.4GHz og 5GHz, som også er en del av det som blir kalt ISM-bånd (Industrial, scientific, medical). Disse områdene er ulisensierte frekvensområder, som alle står fritt til å ta i bruk. Reguleringen av disse frekvensområdene skjer av nasjonale myndigheter. Det er Post- og Teletilsynet som står for denne oppgaven i Norge, hvor 2.4GHz og 5GHz er ulisensierte frekvensområder. Dette betyr at hvem som vil kan ta i bruk disse frekvensområdene uten å ha noen spesiell tillatelse til å gjøre dette, så lenge utstyret de bruker er godkjet.

Det at 802.11 bruker disse ulisensierte frekvensbåndene har både fordeler og ulemper. Den største fordelen er at det er lite som står i veien for at hvem som vil kan ta denne teknologien i bruk. Dette være seg for private hjem, eller store bedrifter. Selv om det er denne tilgjengeligheten til teknologien som har vært en viktig medspiller i å gjøre 802.11 populært, er det ikke denne som står i fokus når vi snakker om sikkerhet. Denne store fordelen til 802.11 er samtidig også en stor ulempe. Pga av det er så enkelt å ta i bruk frekvensområdet, er det mange teknologier som tar dette i bruk. Eksempel på dette er

Bluetooth (som idag stort sett kommer med de fleste mobiltelefoner og tilbehør til disse), trådløse mus og tastatur, trådløse telefoner, babymonitorer. I tillegg til dette slipper også mikrobølgeovner i bruk ut mye elektromagnetiske bølger over hele virkeområdet til 802.11.

Signalstyrke, støy og avstand

Ytelsen i trådløse kanaler avhenger av S/N (signal-støy forhold). Dette forholdstallet viser oss hvor god mottakelse vi har av et signal. S/N avhenger av flere faktorer. Den mottatte signalstyrken er S, som er avhengig av avstand til signalkilden og omgivelser (hindringer osv). N er mengden støy i et område er en sum av termisk støy som kommer naturlig, og støy fra produkter som operer i samme område som 802.11.

Dess mer utstyr som bruker samme frekvensområde, og dess lengre avstand det er mellom de kommuniserende noder, dess lavere S/N forhold får vi. Når S/N minsker, vil også ytelsen til nettverket bli dårlig. 802.11 har flere overføringshastigheter som kan brukes, og vil velge en lavere overføringshastighet hvis det har en dårlig S/N

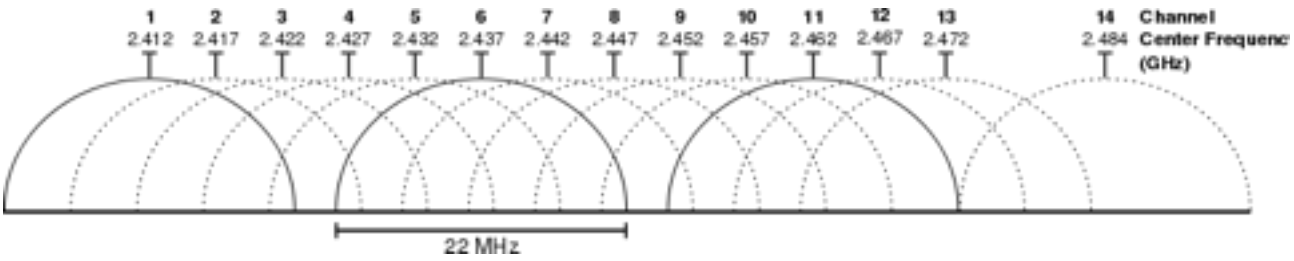
Brukere og kapasitet

802.11 er et delt medium. Til ethvert tidspunkt er det kun en bruker som kan utveksle informasjon. Dersom det er mer enn én bruker, vil disse brukerne «konkurrere» om kapasiteten i nettverket, og hver bruker må vente til mediet er ledig før den kan kommunisere med aksesspunktet.

Kanaler og frekvenser i 802.11

Hver kanal brukt i 802.11 er som tidligere sagt, på 20MHz. Frekvensområdet 802.11b/g bruker er 2.401-2.483GHz. I dette området har man totalt definert 14(13) kanaler. Det er opp til hvert land å bestemme hvilke kanaler som er lovlige å bruke. Man har her en total båndbredde på 82MHz, som skal fordeles på 14 kanaler. Dette gir 5,85MHz/kanal. og vi kan allerede her se at det er endel overlapp på kanalene, og det viser seg at vi kun har 4 (3) kanaler som ikke overlapper hverandre.

Dersom man bruker kanaler i nærheten av hverandre som har overlapp, kan dette fort føre til degradering av signal, lavere S/N, og dermed minsket tilgjengelighet. Dette resulterer enten i nedsatt ytelse, eller totalt tap av tilgjengelighet. Det sier seg da at dersom det er mange 802.11g nettverk i bruk i nærliggende nok områder, vil dette fort tette til frekvensområdet, og degradere ytelsen.



[1] Oversikt over kanaler med tilhørende frekvenser. Merk kanalbredden som her er 22MHz. Dette er pga av at dette er tilpasset amerika, hvor kanalbredden er 22MHz.
http://en.wikipedia.org/wiki/File:2.4_GHz_Wi-Fi_channels_(802.11b,g_WLAN).svg

Når man setter opp et 802.11 nettverk bør man unngå støy og andres signaler ved å ta i bruk ledige frekvensområder i området. Man bør også strebe etter å bruke uoverlappende områder når de geografiske områdene er i nærheten av hverandre for å optimalisere ytelsen.

Dersom frekvensområdet i 2.4GHz blir for fullt, er et alternativ å bruke 802.11a. 802.11a har like stor ytelse som 802.11g (54Mbit/s). I motsetning til 802.11g, som har plass til 4(3) kanaler uten overlapp, har 802.11a plass til 13(12) kanaler uten overlapp. I enkelte land gir også 802.11h utvidelsen oss muligheten til å bruke 12 bånd ekstra. Dette gir oss store fordeler sammenlignet med 802.11b/g.

Dess høyere frekvenser man bruker, dess svakere blir signalet over avstand, og signalet går ikke like lett gjennom hindringer. Dette kan være både en fordel og en ulempe. I en stor bedrift kan man gjerne utnytte dette dersom man trenger mye kapasitet. Man kan da dele nettverket inn i flere opp soner, og dermed øke kapasiteten til nettverket. Dette vil også føre til at det er vanskeligere å koble seg til nettverket utenfor lokalene, noe som kan være en fordel.

Angrep

DoS (Denial-of-Service) angrep på det fysiske lag

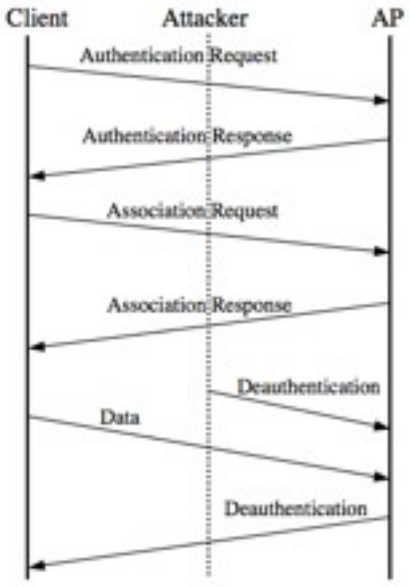
DoS angrep er et angrep som kan utføres veldig enkelt på 802.11. Ved å gjøre S/N dårlig, kan man minske ytelsen til det trådløse nettverket, og i ytterste tilfellet, gjøre nettverket totalt ubrukelig.

S/N minskes lett ved å innføre uønskede signaler inn i området. Dette kan f.eks. gjøres vha en jammer som sender ut støy på et gitt frekvensområde. Dette kan gjøres så enkelt som å sette opp et nettverk i samme frekvensområde, bruke sterke signal, og generere mye trafikk på dette nettverk.

I et DoS angrep er avstand en viktig faktor. Som tidligere sagt er signalstyrken avhengig av avstand. Dette vil også gjelde for et uønsket signal. Et forsvar for et DoS angrep kan dermed være å gjøre det vanskelig for angriperne å komme i nærheten av nettverket.

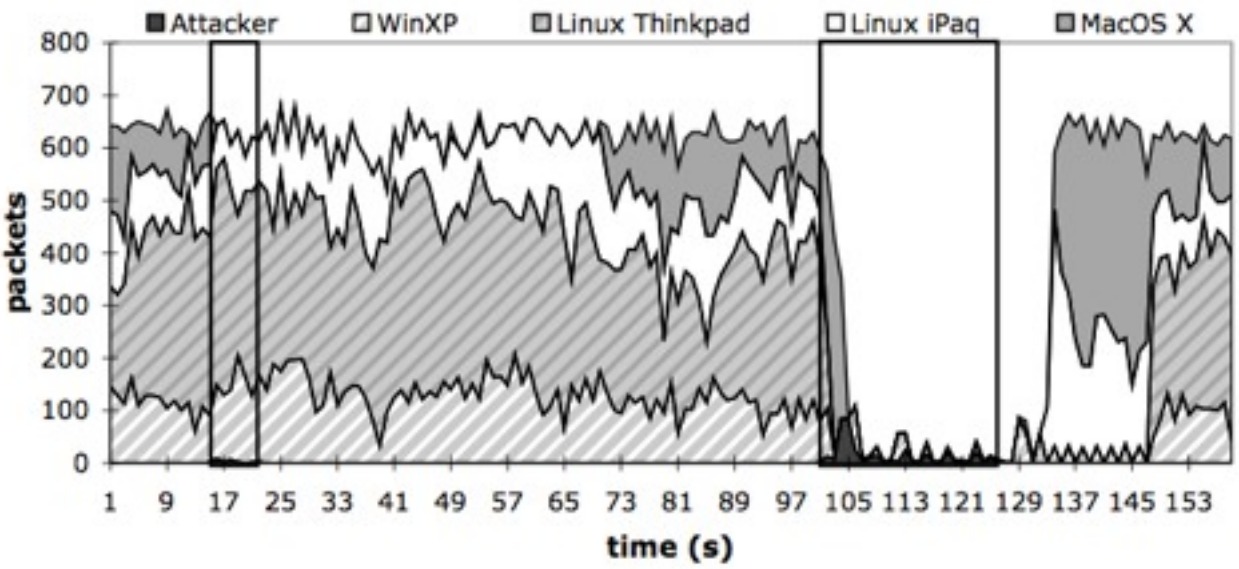
Deauthentication angrep

Et deauthentication angrep utnytter sårbarheter som finnes i MAC-protokollen under en klients oppkoblingen til et trådløst aksesspunkt. For at en forbindelse skal opprettes må aksesspunkt og klient autentiseres for hverandre, før de kan assosieres og informasjon kan utveksles. Det finnes en spesiell melding hvor en av disse kan initiere en deautentisering. Problemet her er at den eneste formen for autentisering av avsender er MAC-adressen, som lett kan spoofes (forfalskes). En utenforstående kan derfor utgi seg for å være en av nodene (aksesspunkt/klient) , og sende en initiering om deautentisering (se figur x). Dersom deautentiseringen er vellykket må klient og basestasjon på nytt gå igjennom prosessen med autentisering. Først etter dette er gjort kan informasjon igjen utveksles. For å hindre at informasjon utveksles, kan angriperen ligge og lytte på kanalen, og initiere deautentisering i det øyeblikk klient og aksesspunkt har blitt assosiert (se figur x).



Ut fra figuren ser vi at klient/aksesspunkt må gjennom 6 steg fra et deauthentication angrep er utført, til en forbindelse igjen er oppe.

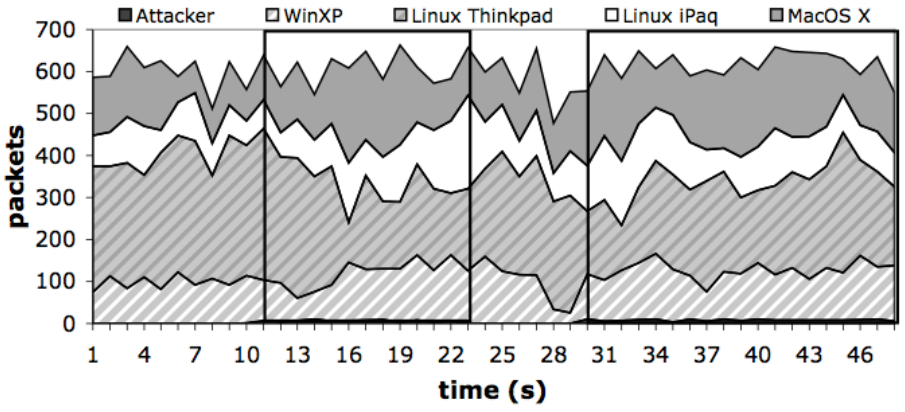
Angriper kan med denne metoden utføre angrep på hvilke klienter den vil, dette være seg enten en klient, flere klienter, eller alle klienter som prøver å koble seg til et aksesspunkt. I.



Figur x - http://cseweb.ucsd.edu/~savage/papers/UsenixSec03.pdf

Figuren viser et deauthentication angrep. I den første rammen(15-23s) utføres et angrep på Mac OS X maskinen. I det andre angrepet (101-127s) utføres et angrep på alle klientene. Vi ser her at et deauthentication angrep er svært effektivt, og at man kan angripe individuelle klienter.

Det finnes ingen standardiserte måter for å stå imot et slikt angrep enda. Arbeid er under utarbeiding i 802.11w, som vi snart kommer tilbake til. En annen måte som har blitt prøvd for å løse dette problemet er å legge inn en forsinkelse i aksesspunktet etter at en deauthentication pakke er mottatt. Dersom det før denne forsinkelsen går ut blir mottatt mer data, vil deauthentication prosessen bli stoppet, og forbindelsen fortsetter som om deauthentication ikke var initiert.
Denne metoden leder dog til andre sikkerhetsrisikoer, som jeg ikke kommer til å gå videre inn på her.



Figur x - http://cseweb.ucsd.edu/~savage/papers/UsenixSec03.pdf
Figuren viser et deauthentication angrep hvor forsinkelsesmekanismen forklart er implementert. Vi ser her angrep først på MacOS X klienten fra 10-22s. Deretter ser vi et angrep på alle klienter som starter på 30s og varer til enden av grafen. Vi ser at forsvarsmekanismen har virket.

Disassociation angrep
En klient kan være autentisert ovenfor flere aksesspunkt, men kun assosiert med ett. Klienten vil kun utveksle informasjon med aksesspunktet den er assosiert med.

Et disassociation angrep er veldig likt et deauthentication angrep. Forskjellen her er at istedetfor for å sende en deauthentication-melding, sender angriper en disassociation-melding. Dette fører til at klienten og aksesspunktet deassosierer seg med hverandre, og må assosiere seg på nytt. Sammenlignet med deauthentication, trenger ikke klienten og aksesspunktet å gjennom autentisering for å gjenopprette forbindelsen på nytt, noe som fører til at det er færre steg for å gjenopprette forbindelsen enn ved et deauthentication angrep (dette ser vi av figur x). Dette betyr at angriperen ved denne type må sende flere pakker for å hindre informasjonsflyt innen et gitt tidsrom enn en angriper som bruker deauthentication angrep.

Angrep på noder i strømsparingsmodus
802.11 klientene har en strømsparingsmodus. Alle pakker som skal bli sendt til klientene blir lagret i en buffer. Antallet pakker som ligger i denne bufferen blir sendt ut fra aksesspunktet ved hjelp av traffic indication map (TIM). Klienten våkner med visse mellomrom, og spør aksesspunktet hvor mye den har liggende i bufferen. Dersom aksesspunktet har noe i bufferen, sender den dette til klienten, og sletter det fra bufferen.

Dette kan en angriper utnytte på flere måter.
- Han kan sende falske forespørsler til aksesspunktet om det har noe informasjon liggende i bufferen. Aksesspunktet vil da sende alt som ligger i bufferen til angriper og tømme bufferen. Når klienten som egentlig skulle hatt dataen som er i bufferen våkner og forespør denne, finnes den ikke i bufferen lenger, og klienten får beskjed om at ingen pakker ligger i bufferen og venter på den.
- Han kan sende falske svar til klienten i det øyeblikket den forespør informasjonen som ligger i bufferen. Angriper gir da klient beskjed om at det ikke finnes noe i bufferen, og klient går tilbake til strømsparingsmodus.
- Strømsparingsmekanismen er også avhengig av synkronisering av TIM (traffic information map) meldinger, og klientene må vite når de skal våkne opp. En angriper kan utnytte dette ved å få klient og akesspunkt til å komme ut av synkronisering de to innehar.

Deauthentication, Disassociation, Strømsparingsmodus
Vi ser at alle disse angrepene benytter seg av samme svakhet i 802.11. Nemlig mangel på autentisering. Angriperen utfører i disse 3 angrepene spoofing, hvor den forfalsker pakker slik at de ser ut som om de kommer fra en annen kilde enn det de egentlig gjør. Dersom 802.11 hadde hatt bedre former for autentisering i autentisering og assosieringsfasen, og i kommunikasjonen rundt strømsparingsmodus uten store svakheter, ville disse problemene vært mye mindre. Disse angrepene er veldig fleksible mtp på hvem man skal angripe, og krever ikke mye datakraft å utføre. Dette kan føre til kritiske situasjoner i 802.11, der klienter kan miste all tilgang til nettverket

802.11w

En standard som nå er under utvikling er 802.11w. Objektet til denne standarden er *«Enhancements to the IEEE 802.11 Medium Access Control layer to provide, as appropriate, mechanisms that enable data integrity, data origin authenticity, replay protection, and data confidentiality for selected IEEE 802.11 management frames including but not limited to: action management frames, deauthentication and disassociation frames.»[1]*

Vi ser at denne standarden adresserer endel av de problemene som vi har diskutert. 802.11w legger inn mekanismer som gjør det vanskelig for angripere å utnytte svakhetene rundt deauthentication og deassociation meldingene. På slutten av kontrollbeskjedene til MAC-laget, legger 802.11w til et MIC-felt (Message Integrity Code). 802.11w kalkulerer MIC feltet ut fra en delt-hemmelighet som kun er tilgjengeglig for autoriserte WLAN brukere. Angriperen kan ikke kalkulere MIC-feltet korrekt siden den ikke har nøkkelen. Dette vil føre til at angriperens forfalskede deauthentication- og deassociation-pakker ikke vil bli godkjent, og angrepene vellykkes dermed ikke.

802.11w er et relativt fersk påbegynt arbeid, som fremdeles er i utvikling. For at 802.11w skal kunne tas ibruk, kreves det oppdatering av alt utstyr som skal kommunisere via 802.11. Dette kan være vanskelig å få til av flere grunner, for eksempel kan eldre utstyr ikke bli oppdatert, slik at man her ikke har muligheten til å bruke 802.11w.

802.11w sikrer mot noen svakheter i 802.11, og bør implementeres dersom man har mulighet for dette. Dette vil fjerne trusselen for å bli angrepet av deauthentication- og deassociation-angrep.

5. Autentisering og aksesskontroll

For å kunne ha kontroll over hva som skjer på nettverket, vil vi søke å ha kontroll over hvem som har tilgang til å koble seg til nettverket. Vi ønsker også å være sikre på nodene i nettverket er de de utgir seg for å være. Og nodene vil gjerne også være sikre på at nettverket det kobler seg til er det rette nettverket. Trådløse nettverk er vanskeligere fysisk kontrollere enn kablede nettverk. På et kablet nettverk kan man i større grad kontrollere hvilke maskiner som er på nettverket, da disse er koblet fysisk til med en kabel.

Den vanligste problemstillingen innenfor dette området er hvordan man sikrer nettverket sitt mot tilgang fra uvedkommende. Og her finnes det mange løsninger. En problemstilling som ikke så ofte er tenkt på, er hvordan man vet at nettverket man kobler til er det man tror det er. Jeg vil prøve å ta for meg litt av begge sidene.

Aksesskontroll

I utgangspunktet er som regel 802.11 nettverk åpne. Alle som vil kan koble seg til nettverket. Vi ønsker ofte å begrense hvem som skal ha tilgang til nettverket. Jeg vil her så på forskjellige måter dette kan gjøres på, deres fordeler og ulemper, og muligens noen former for angrep.

Falske aksesspunkt

En ting brukere må være obs på er «falske» aksesspunkt. Disse «falske» aksespunktene kan enten være en del av et angrep, eller rett og slett være resultat av andre ting. En angriper kan sette inn et aksesspunkt i et område som har samme navn som nettverket. Uten at brukeren vet om dette, kan den assosieres med dette nettverket. Hvis det er en angriper som har satt opp dette falske aksesspunktet, vil han være i stand til å kunne avlytte all informasjon som klienten utveksler.

Skjult SSID

Et 802.11 nettverk er kjennetegnet av en SSID (Service Set Identifier). For å gjøre tilkobling enkelt, blir denne SSID-en vanligvis kringkastet med jevne mellomrom. Dette gjør at klienter kan oppdage nettverket, og øker dermed brukervennligheten. Brukeren kan få opp en liste over de tilgjengelige nettverkene, og lett velge å koble seg til et av disse. Datamaskinen kan også være innstilt på å tilkoble seg et av disse trådløse nettverkene automatisk. En mekanisme som kan gjøre det litt vanskeligere for uønskede brukere å koble seg til dette nettverket, er å skjule SSID-en. Dette gjøres ved at nettverket stopper å kringkaste SSID-en. Klienten må da inneha SSID-en til nettverket for å assosiere seg med dette.

Skjult SSID er en enkel metode for å gjøre nettverket mer utilgjengelig for uvedkommende, men gir oss lite forbedring i sikkerhet. Dersom en angriper lytter på frekvensområdet til 802.11, vil det fort finne mye trafikk til nettverket med skjult SSID, og ha nok informasjon til å koble seg til. Skjult SSID gjør det litt vanskeligere for uvedkommende å koble seg til nettverket. For kompetent personell derimot, er skjult SSID en liten hindring.

Skjult SSID bør absolutt ikke stoles på alene til å hindre uvedkommende å komme inn på nettverket. Dog kan det brukes i forbindelse med andre teknikker.

MAC-filtrering

Som tidligere nevnt, er det MAC-adressen klienten autentiserer seg med ovenfor aksesspunktet. Ved MAC-filtrering lar man bare klienter med visse MAC-adresser autentisere seg mot aksesspunktet. Disse MAC-adressene legges inn på en liste i aksesspunktet. Når en klient prøver å autentisere seg opp mot aksesspunktet, sjekker aksesspunktet MAC-adressen til klienten, og ser om denne finnes i listen. Dersom adressen finnes i listen, godtar aksesspunktet autentiseringen. Men dersom adressen ikke finnes i listen, blir ikke klienten autentisert, og får ikke assosiert seg med aksesspunktet.

MAC-filtrering teknisk enkelt å gjennomføre. Man trenger kun å legge MAC-adressene som skal ha tilgang i en liste. Blir derimot nettverkene store, vil dette være en tungvindt metode. De tillatte MAC-adressene må da legges inn på alle aksesspunktene. Bare å ha kontroll på alle MAC-adressene kan være en omfattende oppgave.

MAC-filtrering er heller ikke veldig sikkert. En angriper kan lytte på nettverket og finne ut hvilke MAC-adresser som får assosiert seg med aksesspunktet. Angriper kan så sette sin egen MAC-adresse til en av disse, og på den måten få tilgang til nettverket. MAC-filtrering er heller derfor ikke en veldig sikker teknikk for å hindre uønskede tilgang til nettverket.

802.1x

Verken skjult SSID og MAC-filtrering har gitt oss noen form for autentisering. Aksesspunkt har ikke hatt mulighet for å se hvem som egentlig kobler seg til. Klienten vet heller ikke at

nettverket den har koblet seg til er det korrekte nettverket. 802.1x er en protokoll som kan løse dette for oss. 802.1x er en av grunnblokkene som er med på å skape 802.11i.

802.1x var en protokoll egentlig beregnet for autentisering på ethernet-nettverk. Under arbeidet med 802.11i ble den derimot utvidet til å også virke på 802.11, og ble en del av 802.11i.
802.1x gir oss autentisering på port-nivå, på det ytterste tilkoblingspunktet for brukeren. Brukeren blir assosiert med porten. Portene i et nettverk som bruker 802.1x kan ha to tilstander. Disse tilstandene har begrenset eller full tilgang. En port er i utgangspunktet i begrenset tilgang. Det er da kun nødvendig informasjon som får lov til å bli utvekslet på porten. Eksempel på tillat trafikk i begrenset modus er EAP (Extensible Authentication Protocol) som brukes til autentisering i 802.1x, eller STP (Spanning Tree Protocol) som brukes til å forhindre lag2-løkker. Tilgangen en har via en port med begrenset tilgang kan tilpasses.
Etter at brukeren har blitt autorisert i 802.1x, går porten over til tilstanden der man har full tilgang. Nå kan brukeren utveksle den informasjon han vil.

802.1x er avhengig av noe infrastruktur. Dette består i all hovedsak av en RADIUS (Remote Authentication Dial In User Service) tjener, og utstyr som støtter 802.1x (802.1x krever ikke at autentiseringstjeneren er en RADIUS-tjener, men det er dette som brukes mest). RADIUS-tjenere har ofte vært brukt som autentiseringstjener hos ISP-er, til VPN-forbindelser, web-tjenere osv. RADIUS-tjeneren autentiserer vanligvis ut fra brukernavn og passord. RADIUS-tjeneren kan f.eks. få denne informasjonen fra SQL, Kerberos, LDAP og Actirve Directory. Dette er løsninger som er mye brukt i større nettverk til forskjellige tjenester, og betyr at autentiseringen kan knyttes opp mot allerede eksisterende løsninger.

802.1x støtter flere EAP-autentiseringsmekanismer, som definerer hvordan autentiseringen foregår. De forskjellige EAP-typene har forskjellig grader av sikkerhet, og krever forskjellig informasjon for autentisering.

Eksempel på EAP-typer:
- EAP-MD5: Her kalkuleres en MD5 sum av brukerens passord. Brukerennavnet sendes med denne MD5-summen, og sjekkes opp mot informasjonen som ligger i autentisersingstjeneren. Dette er ikke en sikker metode på trådløse nettverk, ettersom alle kan sniffe opp dette, og sende den samme informasjonen senere.
- LEAP (Cisco Lightweight EAP): Krever autentisering fra begge sider, og er derfor sikrere mot man-in-the-middle angrep. Cisco-proprietært
- EAP-TLS (EAP med TLS sikkerhet): Bruker asymmetrisk kryptering for å verifisere både autentiseringstjener og klient. Overføringen av denne informasjonen er kryptert i en TLS tunnel. Krever at klienter og autentiseringstjener har sertifikat
- EAP-TTLS (EAP med tunnelert TLS) eller PEAP - Krever et autentiseringstjener-sertifikat, og brukernavn og passord fra klient.

De sikreste løsningene her er EAP-TLS og EAP-TTLS/PEAP. Vi ser at selv om vi bruker 802.1x blir ikke sikkerheten rundt autentisering automatisk god, men den kan bli god.

Å implementere et nettverk som bruker 802.1x krever derfor infrastruktur, mye kompetanse, og noe arbeid. I mange situasjoner (f.eks. i hjemme nettverk, og nettverk i små kontorer) vil dette være uønskelig. 802.11i spesifiserer andre løsninger som også gir oss autentisering, men i tillegg også gir oss konfidensialitet og integritet.

Konfidensialitet og Integritet

Konfidensialitet er kanskje et av de aspektene som er mest diskutert ved trådløs sikkerhet. Og det er med god grunn. Et trådløst medie er lett for uvedkommende å avlytte. Så tilgjengelig som 802.11 utstyr er idag, er det nesten bare for en angriper å komme innenfor rekkevidden til aksespunkt og klient, og sitte og ta imot all informasjonen som utveksles. Det store spørsmålet er hvordan man kan sikre seg at denne informasjonen er konfidensiell. Svaret på dette er kryptering.

WEP -Wired Equivalent Privacy

WEP er en krypteringsmetode som ble innført isammen med 802.11 for å gi økt konfidensialitet. WEP bygger på strøm-chiffer RC4. Krypteringen ligger på MAC-laget, og det er payloaden og CRC-en i pakken som blir kryptert. RC4 er en symmetrisk krypteringschiffer, noe som betyr at samme nøkkel må brukes på alle enheter som skal være med i kommunikasjonen. Nøkkelen i RC4 er på 40bit, men blir utvidet til 64bit med en initialiseringsvektor, dettefor å forhindre at flere chiffertekster blir kryptert med samme nøkkel. Dette er nødvendig for å forhindre angripere å finne statiskiske likheter mellom chiffertekster som har blitt kryptert med den samme nøkkel. I WEP blir initialiseringsvektoren inkludert som rentekst i hver pakke, og det blir derfor lett å finne ut hvilke chiffertekster som er kryptert med samme nøkkel.

Selv om målene med WEP kun var å gi konfidensialitet, tilbydde også denne teknikken integritet.

WEP ble knukket i 2001 av Fluhrer, Mantin og Shamir. De kunne da klare å finne krypteringsnøkkel med en vanlig bærbar datamaskin iløpet av 1-2 timer. Nyere angrep kan klare denne jobben på mindre 60 sekunder. Sett fra et sikkerhetsperspektiv er dette uholdbart.

WPA - Wi-Fi Protected Access

Arbeidet med 802.11i, som inneholdt nye metoder for konfidensialitet, var ikke ferdig på det tidspunktet WEP ble knukket. Dette førte til at WiFi-Alliance, som er et firma som fører til interoperabilitet mellom 802.11 utstyr levert av forskjellige leverandør, innførte en metode for å forbedre konfidensialiteten til 802.11i ble ferdig. Denne standarden ble kalt WPA og er nå en del av 802.11 standarden. Målet med denne metoden var å øke sikkerheten sammenlignet med WEP, samtidig som om man ønsket bakoverkompabilitet med allerede eksisterende 802.11 produkter (via oppdateringer). WPA implementerte også støtte for 802.1x og EAP, og med dette autentisering og muligheten for å få nøkler fra autentiseringstjenester. Dette gir også gjensidig autentisering. I tillegg har WPA en modus kalt WPA-PSK (WPA Pre-Shared Key). WPA-PSK er beregnet for hjemmebrukere. Man har enkelt og greit en forhåndsdelt nøkkel som man manuelt taster inn på klientene som skal være med i nettverket. Dette vil også gi oss autentisering, da man må ha nøkkelen for å komme seg inn på nettverket.

WPA krypterer som WEP RC4 chifferet, men TKIP (Temporal Key Integrity Protocol). TKIP forbedrer svakheten WEP hadde med IV (initialization vector). IV blir nå kalkulert ut fra nøkkelen før den blir brukt i RC4 krypteringen. I tillegg sørger TKIP for at nøkkelen som blir brukt i kryptering forandres underveis. TKIP sørger for den samme nøkkelen aldri blir brukt to ganger på samme plass, og gjør det dermed vanskeligere å utføre statistiske angrep.

WPA er en sikrere protokoll enn WEP. Det har blitt funnet flere hull, men WPA er ikke fullstendig knukket på samme måte som WEP. WPA med TKIP er ikke lenger regnet som sikkert. Og bør derfor ikke brukes om man har muligheten til det.

WPA2

802.11i ble ferdig i 2004. 802.11i inneholdt WEP for å være bakoverkompatibel med den originale standarden. 802.11i introduserte TKIP, og 802.1x, som delvis allerede var innført med WPA. I tillegg innførte 802.11i CCMP som bruker advanced encryption standard (AES). Denne ble innført som en erstatter for WEP og TKIP. I CCMP bruker AES 128-bit nøkler, og 128-bit blokker.

WPA2-CCMP (WPA2 Counter Mode CBC MAC Protocol) kan som TKIP enten bruke 802.1x eller felles nøkler, for autentisering. AES er et mye sterkere chiffer enn WEP, og innehar ikke de samme svakhetene. WPA2-CCMP bruker CBC-MAC (Cipher Block Chaining Message Authentication Code) for integritet.

VPN - Virtual Private Network

En løsning som ble brukt endel før 802.11i og 802.1x ble tatt i bruk på 802.11, var VPN. VPN forbindelser ligger på lag3. Når en VPN forbindelse blir opprettet kobler VPN-klienten til en VPN-tjener. Alle IP-pakker vil bli enkapsulert i nye IP-pakker før de blir sendt inn til tjeneren. Dette betyr at hva som helst kan gjøres med innholdet i IP-pakkene. VPN kan på denne måten tilby autentisering, konfidensialitet og integritet.

Fordeler med VPN er at dette ikke krever støtte i hardware. Dette gjør at oppdateringer fortere kan rulles ut dersom man f.eks. finner hull i chiffer. Man slipper da å vente på at standardene til 802.11 blir oppdatert, slik som skjedde med WEP før 802.11i ble ferdig. En VPN løsning kan også sikre tilgang til internnett fra brukere som kobler til fra andre lokasjoner enn det lokale nettverk.

En VPN løsning vil bruke mer ressurser enn en 802.1x løsning. Man må også sørge for å ha installert nødvendig software på klientene som skal kobles opp mot nettverket. Det er også vanskeligere å konfigurere denne tjenesten. I tillegg vil den bruke mer båndbredde ettersom hele IP-pakken enkapsuleres, dette kan også skape problemer ovenfor enkelte tjenester ettersom at det maksstørrelsen på informasjonen en IP-pakke kan inneholde blir mindre.

Konklusjon

802.11 tilbyr veldig gode metoder for å sikre konfidensialitet, integritet og autentisering. Og dersom dette er satt opp riktig, kan man føle seg ganske trygg. Det har løsninger som passer for både små nettverk, og store kompliserte nettverk. Det finnes derimot en del svakheter når det kommer til tilgjengelighet. Her kan angrep, og støy i frekvensområdene føre til at nettverket ikke er tilgjengelig i det hele tatt, eller sterkt redusert ytelse. Man kan derfor føle seg sikker når man er på godt sikret nettverk, men bør være observant på tilgjengelighetsproblemer, og kanskje ha andre måter å skaffe seg tilgang til nettverket på enn via 802.11.