Sikkerhet i Trådløse Nettverk

Kai G. Palm

Masteroppgave
Master i informasjonssikkerhet
30 ECTS
Avdeling for informatikk og medieteknikk
Høgskolen i Gjøvik, 2007

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Faculty of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Abstract

More and more organizations rely on 802.11 wireless solutions for their mission critical business. Nevertheless there have been numerous security flaws over the years.

With the ratification of the IEEE 802.11i standard things should have improved. A theoretical study reveals that there are many different methods to choose from, and that it is complicated to get a firm grasp on the full picture regarding confidentiality, integrity and authentication in particular. To make things worse most literature is not yet up to date, thus unable to give appropriate and comprehensive guidance on the new standard. Wi-Fi Alliance has issued a list of methods that are mandatory to be Wi-Fi compliant. All known sources fall short on taking this list as well as two-factor authentication into consideration when evaluation the quality of methods offered by the standard.

This paper proposes a security ranking of protocols relevant to confidentiality and integrity in IEEE802.11 as well as taking two-factor authentication into consideration when evaluating the de-facto backend authentication standard for 802.11i, namely 802.1X.

To our knowledge little effort has been done worldwide to investigate what wireless security solutions organizations have chosen and why, thus we have conducted an empirical assessment in 5 major Norwegian organizations on a detailed level to reveal this. Though some of the organizations have utilized modern 802.11i networks, the result clearly shows that other factors than security have been the main drivers when choosing security mechanisms for wireless LANS. The majority had mostly been concerned with compatibility and vendor-specific issues. All interviewees said they had relied on recommendations from consultants and vendors when designing the wireless security solution. Vendors, on the other hand claimed they implemented what the customers wanted.

This report contributes with, as far as we are aware of, the first study in 802.11i security taking two-factor authentication into consideration, as a consequence it is also the first to publish a comprehensive security ranking regarding Wi-Fi compliant 802.1X standards.

To our knowledge it has also made one of the first contributions to a more detailed analysis of organizations motives for the selection of wireless network solutions.

Keywords: WLAN security, network security, authentication, encryption, 802.11i, WEP, WPA, WPA2, 802.11i, security ranking

Sammendrag

På tross av tallrike sikkerhetshendelser har trådløse nettverk utviklet seg til å bli et virksomhetskritisk tilbud i dagens IT-infrastruktur.

Med ratifiseringen av IEEE 802.11 standarden skulle man tro at ting hadde endret seg. Denne masteroppgaven viser, gjennom et teoristudium av sikkerheten rundt 802.11-standarden, at kompleksiteten er omfattende med mange metoder å velge fra. Særlig kartleggingen av metoder for autentisering har vist seg å være omfattende, samt det å vise helheten og sammenhengen mellom de ulike metodene for sikring av WLAN

Gjennom teoristudiet har det vært overraskende å se diskrepansen mellom kravene akademisk litteratur stiller til autentisering i et trådbasert nettverk versus et WLAN etter 802.11 standarden. Mens førstnevnte fremhever to-faktor autentisering som den mest robuste metoden, og da særlig i forhold til tilgang fra fremmede nett, er det oppsiktsvekkende lite fokus på dette i trådløse nettverk.

Det har i dette studiet blitt laget en rangering for godheten av ulike metoder for autentisering, konfidensialitet og integritet i WLAN, og metoder i kombinasjon.

Gjennom intervjuer med nøkkelpersonell i et utvalg norske virksomheter har det vist seg at man ikke benytter seg av de mest robuste sikkerhetsmekanismene som er tilgjengelig for et WLAN.

Det har vist seg at kompleksiteten og utvalget av protokoller i 802.11i er så stort at man i stor grad har støttet seg på ekstern kompetanse, slik at sikreste løsning ikke har blitt valgt. Dårlig kompatibilitet mellom eksisterende utstyr og det mest robuste valget har vært avgjørende for valg av krypterings- og integritetsprotokoll. For autentisering har valget overveiende vært basert på kompatibilitet og et minimumskrav fra diverse føringer som er gitt fra regelverk og organisatoriske forhold.

Rapporten bidrar til, så vidt vi har klart å finne ut, med det første studiet av 802.11i sikkerhet hvor to-faktor autentisering blir tatt med som en del av i vurderingen. Som en konsekvens av dette ser det ut til at dette er den første publiseringen av en rangeringsliste som tar med alle relevante 802.1X autentiseringsmetoder hva Wi-Fi standarden angår.

Så vidt vi vet er dette også et av de første bidrag til en mer detaljert analyse av virksomheters motiv for valg av sikkerhetsløsninger for trådløse nettverk.

Nøkkelord: Trådløse nettverk, WLAN, sikkerhet, nettverkssikkerhet, autentisering, kryptering. 802.11i, WEP, WPA, WPA2, 802.11i, ranking

Forord

Gjennom flere spennende år i sikkerhetsbransjen har jeg hatt sett mange ulike løsninger for trådløse nettverk bli introdusert i markedet. Med særlig interesse har jeg fulgt markedet for sikkerhetsløsningen for trådløse nett, og jeg har hatt en fascinasjon for at på tross av vissheten om problemene, først rundt null-autentisering, deretter rundt WEP, så har virksomhetene utsatt å innføre robuste metoder.

I øyeblikket ser det ut til at RSN-metodene holder mål for sikring av konfidensialitet og integritet. Dersom man velger CCMP vil man antakelig ha tilfredsstillende sikkerhet for årtier fremover. Vi er åpenbart i ferd med å nå et paradigmeskifte når risiko nå har flyttet seg fra selve sikkerhetsprotokollene og over til mer tradisjonell problematikk, som for eksempel tilfredsstillende beskyttelse av selve autentiseringsakkreditivene.

I mitt yrke og de stadige vurderinger vi gjør i sikkerhetssammenheng, så viser det seg gang på gang at kryptering og integritetskontroll på data er det minste problemet. Problemet er så å si alltid knyttet til autentisering, eller opprinnelsesintegritet om man vil. Dette gjelder i høyeste grad også for trådløse nettverk.

Det som først og fremst har overrasket meg er at jeg ikke har klart å finne noen rangering utover min egen, på godheten av metodene som er tilgjengelig for sikring av WLAN. Dernest har det overrasket meg hvor komplekst rammeverket har vært å sette seg inn i, og hvor lite kongruent og komplett forskningsmaterialet, og ikke minst lærebøker og leverandøranbefalinger er på området. Det har derfor vært et tungt og omfattende litteraturstudie.

Det har også vært overraskende at det ikke har vært mer tilgjengelig empirisk materiale på detaljnivå hva krypterings og autentiseringsmetoder angår. Mørketallsundersøkelsen nøyer seg med å undersøke hvorvidt virksomhetene i det hele tatt krypterer eller ikke. Det spesifiseres ikke metode. På den annen side ser jeg at det vil være svært vanskelig å få valide svar på dette detaljnivået dersom man gjør dette som kvantitative undersøkelser.

Jeg har, gjennom innsikten som teoristudiene i henhold til forskningsspørsmål 1 har gitt valgt, å endre forskningsspørsmål 2 til noe annet enn det som var opprinnelig tenkt.

På denne måten ble hovedfokus for veiledning i forskningsspørsmål 2 og 3, metodevalg, intervjuguide og analyse av dataene i stedet for det opprinnelige eksperimentet som var forespeilet i det opprinnelige forskningsspørsmål 2.

Jeg takker veileder Jan Arild Audestad for god støtte underveis, og forståelsen for at slike ting kan skje.

Takk også til min unike familie for støtte, og til verdens beste arbeidsgiver Kongsberg Maritme. Så lange netter hadde ikke vært mulig uten dere!

Sandefjord, 31 oktober 2007
Kai G Palm

Innholdsfortegnelse

Liste over figurer

Liste over tabeller

1. Innledning

1.1. Problembeskrivelse

I dagens informasjonssamfunn er trådløs tilgang til virksomhetsnettverk nærmest et krav.

På tross av at trådløs nettverkstilgang som oftest starter som et supplement til det kablede virksomhetsnettverket, for eksempel som et tilbud om ren internett aksess, viser det seg ofte at tilbudet etter kort tid materialiserer seg som et virksomhetskritisk tilbud for tilgang til alle virksomhetens nettverksressurser. Dette er en tilgang som tradisjonelt kun har blitt tilbudt fra kablet infrastruktur innenfor virksomhetens bygningsmessige og informasjonsteknologiske skallsikring.

Denne logiske opphevingen av effektiv skallsikring byr på nye utfordringer.

Utbredelsen er av trådløse nettverk (WLAN) er stor. I henhold til [VAC] har pr 2006 48 % av alle virksomheter i USA med flere enn 200 ansatte rullet ut WLAN. I Norge viser Mørketallsundersøkelsen [NSR] for 2006 at over 40 prosent av norske virksomheter i dag tilbyr trådløse nettverk. Samtidig viser undersøkelsen at en tredel av virksomhetene får *alvorlige problemer* allerede etter en times driftavbrudd.

En mindre vitenskaplig rapport fra 2005 utarbeidet en taxisjåfør som hadde vært utstyrt med GPS, PC og programvare i bilen viste 45 000 trådløse nettverk i en 50 km radius rundt Oslo. Rapporten baserte seg på taxikjøring over 68 000 kilometer i en periode på 4000 timer (tilsvarer 533 normale arbeidsdager) [NUUG]. Fenomenet er utbredt og kalles gjerne ”wardriving”.

Utbredelsen av WLAN akselererte dramatisk rundt årtusenskiftet. Primære drivere for dette var blant annet enkel implementering, dramatisk reduksjon av prisene[HUR1], samt at den største produsenten av mikroprosessorer integrerte støtte for teknologien i sine produkter [STMLD17].

Trenden ser også ut til å fortsette, blant annet kan [WIFI] melde at salget av trådløse adaptere/chipsset på verdensbasis har hatt en vekst på 200 millioner i 2006. Prognoser fra samme undersøkelse viser at salget er ventet å stige jevnt frem mot 600 millioner enheter frem mot år 2010.

Stor utbredelse på kort tid, og forventninger om fortsatt vekst, førte til at interessen for sikkerhetsmekanismene, og ikke minst ønsket om å bryte disse økte raskt. Paradoksalt nok har systemeierne i liten grad sikret sine WLAN. Totalt sett viser [NUUG] at ca 50-55% av de trådløse nettene i Oslo er helt uten kryptering. En relativt analog undersøkelsen, men i langt mindre skala, viste at 40 % av alle WLAN i Bergen var åpne [HOL].

Selv om datagrunnlaget i [NUUG] er enormt, og i høyeste grad sier noe om utbredelsen i området hvor dataene er samlet inn, sier verken denne eller

undersøkelsen fra Bergen noe om hva slags sikringstiltak som er gjort. Datainnsamlingens natur gjør at disse undersøkelsene heller ikke skiller på virksomheter og privatpersoners nettverk, utover at den Oslo-baserte undersøkelsen peker på at andelen krypterte nettverk var høyere i nærings- enn boligområder.

Tallene fra Mørketallsundersøkelsen [NSR] er hentet fra norske virksomheter, men heller ikke denne undersøkelsen sier noe om hvilke sikringstiltak som er tatt i bruk utover spørsmålet om virksomhetene krypterer eller ikke. Antall som krypterer WLAN-trafikken i denne undersøkelsen varierer fra 12 prosent for de minste bedriftene, til drøyt 50 prosent for de med over 500 ansatte.

I en undersøkelse [RSA1] i 2006 utført på oppdrag av sikkerhetsselskapet RSA blant virksomheter i San Francisco og Frankfurt viste at cirka en tredel av virksomhetsnettverkene var usikret. Oppsiktsvekkende hadde henholdsvis 31 og 28 prosent av disse også standardverdier på det trådløse nettverksutstyret. Sistnevnte svekker sikkerheten ytterligere og åpner for muligheten til en rekke svært enkle og effektive angrep.

[NUUG] og [HOL] sier altså noe om utbredelsen av kryptering på generelt nivå i et geografisk angitt område, mens [NSR] og [RSA1] gir tilsvarende kunnskap i bedriftsmarkedet. Ingen av undersøkelsen sier imidlertid noe om hva slags sikringstiltak som er iverksatt, utover det faktum om hvorvidt nettverkene er kryptert eller ikke.

Sikring av konfidensialitet/integritet og autentisering i WLAN, er fokus i vår rapport. Det finnes gode og mindre gode metoder for dette, kalt henholdsvis Robuste security networks (RSN) og pre-RSN metoder. Det har vært svært vanskelig å finne undersøkelser på et detaljnivå som viser disse valgene, men et paper fra 2006 [BIT] med gjennomgang av 400 WLAN i London og 2539 i Seattle-området viser at svært få nettverk benytter seg av god sikring; RSN. I likhet med de fleste andre undersøkelser vi har sett ligger prosentandelen for krypterte nett på i overkant av 50 %. [BIT] viser imidlertid at av disse så benytter fremdeles henholdsvis 78 og 85 % WEP-kryptering, dvs mindre gode pre-RSN metoder. Undersøkelsen slår fast at selv om leverandører anbefaler oppgradering til RSN metoder er det svært få som lytter til rådene.

Selv om pre-RSN metoden er bedre enn ingen sikring i det hele tatt, så har disse metodene gjentatte ganger vært dokumentert som usikre, noe også denne rapporten viser. Hva er så årsaken til at så mange virksomheter velger å ikke sikre sine nettverk tilfredsstillende. Er man ikke klar over risikoene man introduserer ved å introdusere trådløse nettverk, og at man ikke ser på seg selv som et mål?

En amerikansk undersøkelse gjennomført av CSI/FBI [CSI06] tilsier noe annet. Frykten for sikkerhetsbrudd i, eller i tilknytning til trådløse nettverk viser seg å være tilstede. I undersøkelsen har respondentene, som er et utvalg sikkerhetsansvarlige i amerikanske virksomheter, forsøkt å predikere hva de ser som de mest kritiske sikkerhetsaspektene de nærmeste 2 årene.

1. Beskyttelse av data autentisering, kryptering
3. Identitetstyveri og konfidensialitetsbrudd

5. Aksesskontroll
7. WLAN

Vi ser at WLAN i seg selv er på en 7. plass, isolert sett virker ikke dette høyt, men dersom man ser det i sammenheng med plassene 1, 3, 5 er dette trusler som reelt sett har et enormt potensial til å materialisere seg som en følge av dårlig WLAN-sikkerhet.

Videre viser denne og foregående undersøkelser [CSI05], [CSI06] at siden 2004 har årlig mellom 14 og 17 prosent av respondentene avdekket sikkerhetshendelser og/eller –brudd knyttet til WLAN-sikkerheten. 78 prosent sier også, i 20006, at nettverkssikkerhet er det området hvor det er nødvendig å investere tyngst i nær fremtid.

Dette kan vise seg å være et klokt resonnement. Det er åpenbart at brudd på nettverkssikkerheten, også den trådløse kan ha store økonomiske konsekvenser. En amerikansk butikk kjede har, etter brudd på WLAN-sikkerheten hatt enorme økonomiske tap. I rene kostnader, resultat av eventuelle søksmål unntatt, anslås beløpet til omkring 1 milliard dollar. Se for øvrig **4.3**

I april 2007 ble det gjennomført en undersøkelse [SYM2] med 300 IT-ansvarlige i norske små og mellomstore bedrifter (SMB-markedet). I undersøkelsen går det frem at trådløst nettverk topper listen over teknologier som virksomhetene frykter skal føre til sikkerhetsproblemer. Videre viser undersøkelsen at bare halvparten av deltakerne i undersøkelsen mener de har ”sikre IT-systemer”. En av fire IT-ansvarlige føler at det viktigste hinderet for sikkerhet i bedriften er deres egen mangel på tilstrekkelig kunnskap, og nesten like mange oppgir tidspress som sikkerhetshinder.

Undersøkelsen er gjennomført på oppdrag av en virksomhet som omtaler seg som ”verdensledende innen løsninger som gjør det enklere for privatpersoner og bedrifter å garantere informasjonssikkerhet” (…). På virksomhetenes nettsted kommenteres resultatene av undersøkelsen slik: ”Resultatene fra undersøkelsen bekrefter det vi har sett lenge, at mange savner kunnskap om hvordan de kan sikre datasystemene sine. Derfor har vi nå lansert en ny utgave av boken ”Et sikkert IT-miljø”. Boken er på norsk, skrevet for ikke-eksperter og gir praktiske råd og tips til hvordan bedriften kan sikre sine informasjonsverdier.”

Av konkrete råd fra boken [SYM1], som er fritt tilgjengelig fra virksomhetens nettsted, kan vi lese at anbefales det å beskytte virksomhetens trådløse nettverk gjennom å sørge for fysisk sikkerhet og plassere trådløse aksesspunkter midt i bygget. Dette i tillegg til å bruke WEP for å sikre datakommunikasjonen.

Vi har allerede kommentert at det er marginal sikkerhetsmessig gevinst i WEP-kryptering og kanskje ennå mindre i form av selektiv antenneplassering. Ingen av metodene er egnet til å beskytte bedriftsnettverket lengre enn maksimalt 60 sekunder.

I litteraturen og fagpressen har vi funnet talløse eksempler på villedende informasjon og mindre gode råd. Mye av dette skyldes åpenbart at litteraturen er foreldet, men det finnes også eksempler på at oppdaterte artikler i anerkjente medier man tradisjonelt har hatt tillit til også feiler på å gi relevante råd. Majoriteten av fagpersoner vil

naturligvis umiddelbart forstå at rådet som er gitt over er dårlig. Betenkelig er det derfor at målgruppen for "Et sikkert IT-miljø" er det utgiveren omtaler som "ikke-eksperter". Disse kan jo tenkes å følge rådet. Nedenfor følger et siste eksempel for å vise at selv om man har forstått at WEP er uegnet, så er det også mulig å fremstå med en viss autoritet og fremdeles feile på å gi relevante råd.

I et anerkjent norsk fagtidsskrift fra medio 2006, under vignetten "Forstå trådløs sikkerhet" [NOK], anbefaler en anerkjent skribent og lærebokforfatter bruk av EAP og 802.1X for autentisering i WLAN. Dette er isolert sett et godt forslag og grunnlaget for god autentisering i et RSN. Imidlertid anbefaler han i denne konteksten å bruke den Cisco-proprietære protokollen LEAP. Dette på tross av Cisco Systems i et sikkerhets varsel[1] datert 7. august 2003 advarer om at LEAP var funnet sårbar for ordliste angrep. Sikkerhetsvarselet kom som et svar på Joshua Wrights demonstrasjonen av Asleap på Defcon samme dag [WRI03]. Cisco Systems har etter dette anbefalt å benytte andre metoder enn LEAP.

Det mest oppsiktsvekkende med denne artikkelen er foruten at man ikke adresserer en vesentlig sårbarhet som allerede hadde vært kjent i 3 år, det faktum at LEAP presenteres som eneste alternativ for autentisering i et 802.1X RSN-miljø. Langt mer robuste og standardiserte EAP-metoder eksisterer, og kan uten videre brukes under samme infrastrukturen som kreves av en LEAP-løsning.

Vi ser altså at utbredelsen og angrepene på trådløse nettverk er omfattende, og at prognosene tilsier at antallet øker for hvert år.

Med introduksjonen av 802.11i og kravet til RSN, er det nå mulig å oppnå bedre WLAN sikkerhet enn noensinne. Imidlertid er det mange tilgjengelige metoder i standarden og vi er av den oppfatning av at litteraturen er lite oppdatert, oversiktlig og etterrettelig. Som en konsekvens av dette har det ikke vært mulig å finne en autoritativ rangering av metodenes godhet.

Det viser seg dessuten at det finnes begrenset kunnskap om hvilke metoder virksomheter bruker, ettersom de fleste undersøkelser er lite vitenskapelige og ikke gir detaljerte svar på hvilke trådløse sikkerhetsmekanismer som er valgt, og dermed heller ikke på hvilket grunnlag beslutningene er fattet.

Konklusjonen og prosjektets berettigelse bunner altså i at informasjon som er tilgjengelig i markedet er dårlig kvalitetssikret og lite samsvarende med dagens krav. Årsaken kan se ut til å være manglende kunnskap, dårlig rådgiving og vanskelig tilgjengelig litteratur.

Dette fører oss frem til følgende overordnede problemformulering

Finne beste metode for sikring av trådløse nett, gjennom et teoristudium, og se i hvilken grad dette er samsvarende med valg gjort i et utvalg norske virksomheter som bruker 802.11 for å gi tilgang til virksomhetens ressurser.

[1] Eng: Security Bulletin

1.2. Forskningsspørsmål, bidrag og forventede funn

Denne rapporten setter søkelys på hvilke metoder som finnes for å sikre et WLAN i henhold til definerte standarder, og rangerer disse. Vi ser også på et lite utvalg norske virksomheter, og forsøker blant annet å finne hva som har vært den primære driveren for deres valg av sikring for trådløst nettverk. Problemformuleringen i 1.1 operasjonaliseres med følgende forskningsspørsmål:

- Kan vi rangere metoder for sikring av WLAN?
- Hvilke metoder for sikring av WLAN blir brukt av et utvalg virksomheter?
- Hvorfor har virksomheten valgt denne løsningen?

Rapporten bidrar hovedsakelig til 3 ting:

1. Tilgjengeliggjøre en rangering av relevante sikringsmetoder i hht etablerte standarder
2. Samle relevant informasjon om valg av WLAN sikkerhetsprotokoller på ett sted
3. Gi en detaljert beskrivelse av sikkerhetsløsningene, og bakgrunnen for valget av disse i noen større norske virksomheter

Basert på problemformuleringen og forskningsspørsmålene har vi følgende antagelser:

- Basert på et teoristudium, kan det identifiseres en rangering av robustheten av ulike sikringsmetoder for WLAN.

Basert på intervjuer i 5 større norske virksomheter:

- Virksomhetene tror de har valgt ”den sikreste løsningen”
- Valgene er ikke samsvarende med min rangering
- Det finnes andre drivere som har blitt lagt til grunn for valgt løsning enn sikkerhet
- Valget er basert på anbefalinger
- Valget samsvarer ikke med hvordan man behandler tilgang fra andre eksterne nett

1.3. Avgrensninger

Rammene som er tilgjengelige omkring denne rapporten gjort det nødvendig å gjøre en del avgrensninger. Vi fokuserer kun på det som i dagligtale kalles WLAN, eller trådløst nettverk, og da med fokus på større virksomheter. Selv om mange av problemstillingene kan ha direkte overføringsverdi til hjemmebrukere vil ikke denne problematikken bli behandlet spesielt her. Fokus er på trådløse nettverk realisert i form av radiosignaler i 2,4Ghz båndet i henhold til IEEE[2]802.11b og IEEE802.11g standarden[3].

[2] IEEE – (utt: ai-trippel-i) The Institute of Electrical and Electronics Engineers

[3] Problembeskrivelsen angående konfidensialitet og integritet vil åpenbart være generaliserbar til 802.11a (5GHz) og senere 802.11n (2,4 og/eller 5GHz) når denne blir ratifisert (tentativt 4 kvartal 2008).

Vi berør med andre ord ikke teknologier som for eksempel infrarøde personlige nett IrDA, ETSIs[4] HIPERLAN, Wireless MAN/Wi-Max [IEEE802.16] trådløse WPAN (Wireless Personal Area Network) i henhold til [802.15] standarden, for eksempel blåtann

Vi berører heller ikke kommunikasjon som baserer seg på bruk av det mobile telenettet som bærer for eksempel GSM og UMTS.

Videre henvises det til annet arbeid for referanser, for eksempel [802.11] for en teknisk diskusjon av grunnleggende radiokommunikasjon på det fysiske laget fungerer.

Utvalget som deltar i den empiriske undersøkelsen er utelukkende fra den øvre delen av bedriftsmarkedet, dvs virksomheter som har over 1000 potensielle WLAN brukere, samt har en egen IT-organisasjon og opererer i offentlig eller privat sektor. Små virksomheter eller privatpersoners WLAN-løsninger er ikke i fokus. Dette forhindrer allikevel ikke at anbefalingene og metoden fra teoristudiet også vil kunne ha relevans for disse.

Trådløse nett i henhold til 802.11 standarden kommer i 2 operasjonsmodi, Adhoc modus og infrastructure modus. Oppgaven fokuserer på sistnevnte. Som en følge av dette blir heller ikke problematikken omkring nøkler som benyttes for broadcast og multicast i WLAN etter 802.11 i standarden berørt.

802.11i standarden spesifiserer ikke autentiseringsmetode eller type for enterprise modus, i stedet inviterer den til å bruke det allerede etablerte rammeverket 802.1X [802.1X]

Innenfor 802.1X er det et utall EAP-typer å velge mellom. Vi begrenser oss til å se på et relevant utvalg, nemlig EAP-TLS, EAP-PEAP i variantene GTC og MS-CHAP2, samt EAP-TTLS/MS-CHAP2. I tillegg diskuteres en proprietær protokoller fra Cisco Systems; LEAP. De fire førstnevnte er valgt fordi det er et krav dersom enheten skal kunne sertifiseres av Wi-Fi Alliance. Sistnevnte har stor utbredelse og er derfor tatt med på tross av at den er proprietær og lukket. Ytterligere argumentasjon for valget av nettopp disse er gitt i kapittel 4.14 ff.

Wi-Fi Alliance ble etablert i 1999 som en uavhengig interesseorganisasjon for produsenter av trådløst nettverksutstyr. Organisasjonen markedsfører 802.11 nettverk som ”Wi-Fi”. Merkingen er et resultat av at produsentene har tatt initiativ et system som skal garantere for kompatibilitet, samt at det møter et minimumskrav til standardiserte sikkerhetsprotokoller.

[4] ETSI - European Telecommunications Standards Institute

I en brytningstid mellom vissheten om at det var grunnleggende sikkerhetsmangler i [802.11-1999] og behovet for trådløse løsninger, vokste det frem et stort marked for trådløse løsninger basert på tradisjonelle VPN mekanismer. Kompleksitet i protokollen, manglende støtte for forflytting mellom aksesspunkter[5] [WON], samt krav til klientprogramvare har gjort disse løsningene lite skalerbare og relativt kompliserte, både fra et teknisk og administrasjonsmessig ståsted. Flere av de mest utbredte protokollene på dette området har dessuten kjente sårbarheter.

På grunn av dette er det vår klare oppfatning at slike løsninger vil måtte vike nå som 802.11i standarden begynner å bli kjent og rullet ut. Standarden vil, etter vårt syn, gjøre disse WLAN løsningene basert på VPN overflødige i de aller fleste miljøer. Som en konsekvens av dette, samt at området er for omfattende og mangefasettert til å bli behandlet innenfor oppgavens rammer blir ikke løsninger som baserer seg på VPN behandlet videre her.

Som i annet sikkerhetsarbeid er det som kjent flere tiltak enn kryptering og autentisering som må ivaretas. I sikkerhetssammenheng har det tradisjonelt vært vanlig å betrakte sikkerhetstjenestene konfidensialitet, integritet og tilgjengelighet. Sistnevnte har ikke vært innenfor TGi[6] sitt mandat å utrede, og er således ikke behandlet utover på et generelt nivå i kapittel 4.3. Det må nevnes at motstandsdyktighet mot tjenestenekt-angrep på trådløse nettverk er en høyst relevant problemstilling, særlig ettersom trådløse nettverk er i ferd med å utvikle seg til virksomhetskritisk infrastruktur.

Det er også sentralt at for å tilfredsstillende kunne sikre datakommunikasjon trenger man flere tiltak enn de som kan leveres i en sikkerhetsprotokoll.

Autoriteter velger ofte å skille mellom tekniske, organisatoriske og administrative tiltak [NIST800-48]. Denne rapporten fokuserer utelukkende på tekniske tiltak.

I tillegg kommer problematikken omkring fremmede trådløse nett, og hvordan sikre klienten og datakommunikasjon på disse fremmede nettverkene. Problematikken er viktig men behandles ikke her.

Her begrenser vi oss imidlertid til å se på tekniske metoder i form av ulike protokoller for kryptering og autentisering, samt diverse ”lavnivåtiltak”.

For å få en så god sikring av den trådløse infrastrukturen som mulig vil det være helt nødvendig med ytterligere sikringstiltak i dybden, slik som for eksempel brannvegger og antivirus på nettverksnoder, planer for oppdatering av programvare (patching), innbruddsdeteksjons programvare (IDS), brukeropplæring og sikkerhetspolicyer. Det finnes flere referanser for dette arbeidet, [NIST800-97] anbefales for en oversikt.

Avslutningsvis i dette arbeidet blir det vist til noen konkrete sårbarheter i ulike implementasjoner. Selv om sårbarhetene i selve sikkerhetsprotokollene vil være

[5] Eng: Roaming

[6] Task Group i – grupperingen som har jobbet frem IEEE standarden 802.11i

uavhengige av operativsystemvalg, har praktiske implementsjonsspesifikke scenarioer på klient-/supplikantsiden blitt avgrenset til Microsoft Windows.

1.4. Leserveiledning

Denne rapporten består av en teoretisk og en empirisk del. Den teoretiske delen er av relativt teknisk, blant annet med en del formalia rundt informasjonssikkerhet og trådløse nettverk som fenomen. Det gis beskrivelser av angrepsmetodikk, protokoller og standarder. Dette er nødvendig for å kunne gi et helhetlig bilde og for å kunne finne og adressere relevante problemområder i et eksplorativt studie. Selv om bare de relvante delene i forhold til vår problemformulering er tatt med kan stoffet virke overveldende for lesere med liten teknisk bakgrunn og interesse. Det er derfor lagt opp til at det vil være mulig få tilgang til hovedfunnene gjennom å lese det utarbeidede utvidede sammendraget[7] kapittel 1.5, for rangering og beskrivelse av de tekniske funnene uten de tyngste detaljene.

For en drøfting av funnene i rapportens empiriske undersøkelse vises det til kapittel 6.

Resten av rapporten er organisert som følger:

Kapittel 4 og 5 – Teoristudium med konklusjon besvarer forskningsspørsmål 1 og Kapittel 6 og 7 besvarer forskningsspørsmål 2 og 3.

1.5. Utvidet sammendrag

På bakgrunn av årsaker som er beskrevet tidligere har det i denne rapporten blitt utarbeidet rangeringslister for godheten av sikringstiltak som tilbys innenfor de facto standarden til Wi-Fi alliance og den offisielle IEEE standarden 802.11i. Det vises først til en liste for rangering av konfidensialitets- og integritetstiltak, deretter en tilsvarende rangering for autentisering.

1.5.1. Rangering av konfidensialitets- og integritetsmekanismer

WPA og WPA2 er tungt markedsførte og innarbeidede begreper fra Wi-Fi alliance. Selv om dette ikke det er helt korrekt i henhold til 802.11i-standarden, kan en leser som er kjent med disse begrepene anta at WPA2 er ekvivalent med CCMP og WPA er ekvivalent med TKIP.

Vår rangeringen av tilgjengelig metoder for konfidensialitet og integritet er som følger; beste først:

1. CCMP
2. TKIP
3. WEP
4. Diverse Lavnivåtiltak (se 4.7 for detaljer)

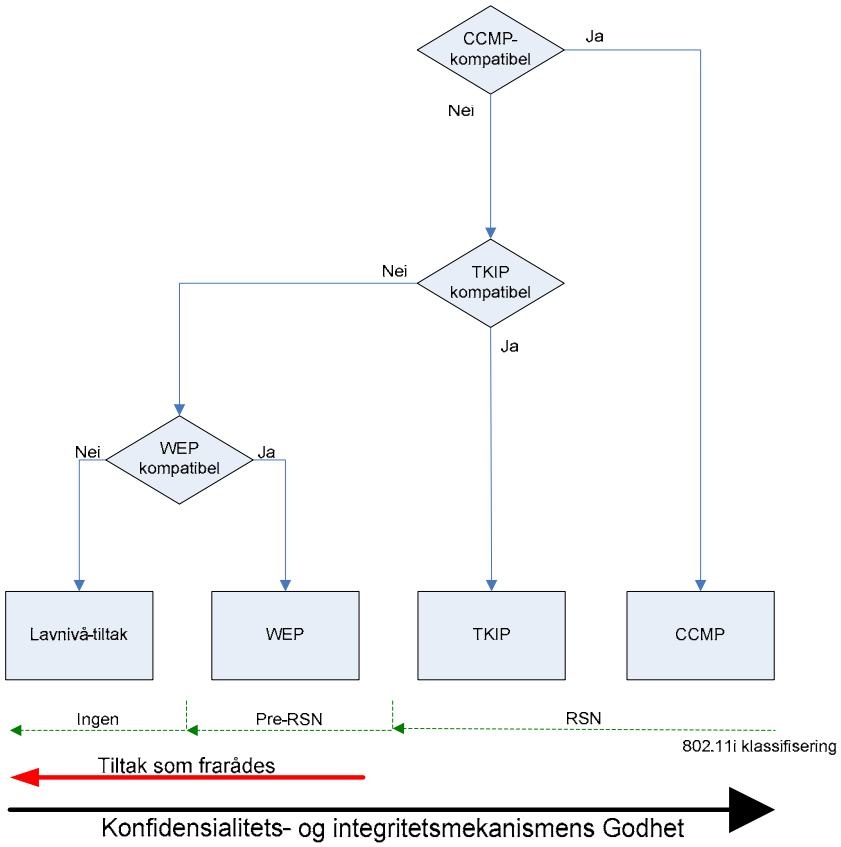
Med bakgrunn i et omfattende teoristudie konkluderer vi med at CCMP, som bygger på anerkjente prinsipper for konstruksjon av en sikkerhetsprotokoll, antakelig vil være sikker nok i årtier fremover. TKIP kan også anbefales i en overgangsperiode, men

[7] Eng: Executive summary

ettersom den baserer seg på feilfiksing av alle kjente svakheter i den usikre WEP-protokollen, kreves det at man følger utviklingen nøye. Protokollens natur gjør at dersom en av byggesteinene i TKIP kompromitteres så vil sikkerheten i protokollen som helhet falle som et korthus. Brudd på konfidensialitet vil også gi brudd på aksesskontroll og autentisering, en svakhet som TKIP har arvet fra WEP.

WEP-protokollen knekkes nå på under 60 sekunder, uavhengig av mengden legitim datatrafikk, og bør ikke lengre benyttes. På tross av at 802.11i standarden mener at denne kan benyttes i en migreringsfase mot et RSN er vi ikke av samme oppfatning. Bakgrunnen er enkel, vi antar at en migreringsfase varer lengre enn det minuttet det tar å kompromittere sikkerheten. I enkelte sammenhenger hevdes det at man ved bruk av diverse lavnivåtiltak, som selektiv antenneplassering, bruk av statiske IP-adresser og skjuling av nettverksnavn (SSID) vil kunne få et høyere sikkerhetsnivå. I denne rapporten konkluderer vi imidlertid med at slike tiltak har liten eller ingen verdi i seg selv. Faktisk viser det seg at skjuling av SSID muliggjør en ny type angrep på klientene, såkalt SSID cloaking angrep.

Den våkne leser vil selvsagt stille seg spørsmålet om hvorfor ikke alle benytter CCMP for konfidensialitet og integritet. Svaret er dessverre at eldre maskinvare ikke kan brukes sammen med CCMP. Selv om man har maskinpark som støtter CCMP kreves det i et Windows XP miljø manuell nedlasting og installasjon av en programvareoppdatering. Denne oppdateringen tilbys ikke gjennom Microsofts automatiserte oppdateringstjenester (Windows Update og lignende). For større organisasjoner kan det være en betydelig administrativ byrde å rulle ut en slik oppdatering. Eldre trådløse aksesspunkter støtter heller ikke CCMP. TKIP derimot tilbys som en del av Windows XP servicepack 1, og senere. TKIP har altså vært tilgjengelig som for XP siden september 2002. De fleste aksesspunkter vil dessuten kunne tilby TKIP dersom man henter inn programvareoppdateringer. Som vi ser er det flere forhold som må tas i betraktning. For oversiktens skyld har vi utarbeidet et enkelt flytdiagram for valg av mekanisme.



Figur 1 Konfidensialitet og integritetsmekanismer i WLAN

X-aksen speiler rangeringslisten ovenfor og diagrammet kan leses slik; Dersom hele virksomheten er CCMP kompatibel velger man denne metoden. Dersom ikke hele virksomheten er CCMP-kompatibel stiller man seg spørsmålet om de som ikke er CCMP-kompatible kan ta i bruk TKIP. Dersom dette er tilfelle kan man sette opp det trådløse nettverksutstyret til å tilby både CCMP og TKIP, og det er opp til brukerne å velge. I litteraturen er dette ofte vist til som CCMP/TKIP-mixed mode. For metodikkens del omtales den her kun som TKIP. Dersom man ikke er kompatible med CCMP eller TKIP er WEP eller lavnivåtiltak eneste mulighet. Med dette utfallet vil anbefalingen være å investere eller oppgradere, ettersom både WEP og lavnivå tiltak ikke gir tilfredsstillende sikkerhet.

1.5.2. Rangering av autentiseringsmekanismer

Valg av riktig autentiseringsmetode er helt avgjørende for sikkerhetsnivået i et WLAN. På et overordnet nivå er det to prinsipielt forskjellige løsninger, nemlig personlig modus" og "virksomhetsmodus[8]". Førstnevnte krever at hele organisasjonen deler én nøkkel, nøkkelen er oftest relativt statisk og gjør nøkkeladministrasjon og hemmelighold utfordrende. Sistnevnte baserer seg på gjenbruk av autentiseringdata[9]

[8] Wi-Fi Alliance omtaler dette som henholdsvis Personal Mode og Enterprise Mode

[9] Med autentiseringsdata forstås her dataene som bekrefter en identitet, f eks en antatt unik kombinasjon av brukernavn og passord.

fra den samme brukerdatabasen[10] som benyttes på virksomhetens trådbaserte nettverk. Fra et infrastrukturelt ståsted vil personlig modus skille seg fra virksomhetsmodus ved at sistnevnte krever en RADIUS-server for å videreformidle autentiseringsdata til virksomhetens brukerdatabase.

Å velge autentiseringsmekanisme i et trådløst nettverk er en utfordrende oppgave som krever en grundig analyse av sikkerhetsbehovet, dette må avstemmes mot kostnadene ved de ulike løsningene. Vi tror rangeringslisten, og det utvidede flytdiagrammet nedenfor vil bidra til en oversikt over hvilke metoder som er tilgjengelige og godheten av disse, samt bidra med noen innspill til andre faktorer som bør tas i betraktning før valget fattes. Generelt sett der det ønskelig fra et sikkerhetsståsted å komme seg "så langt til høyre" som mulig.

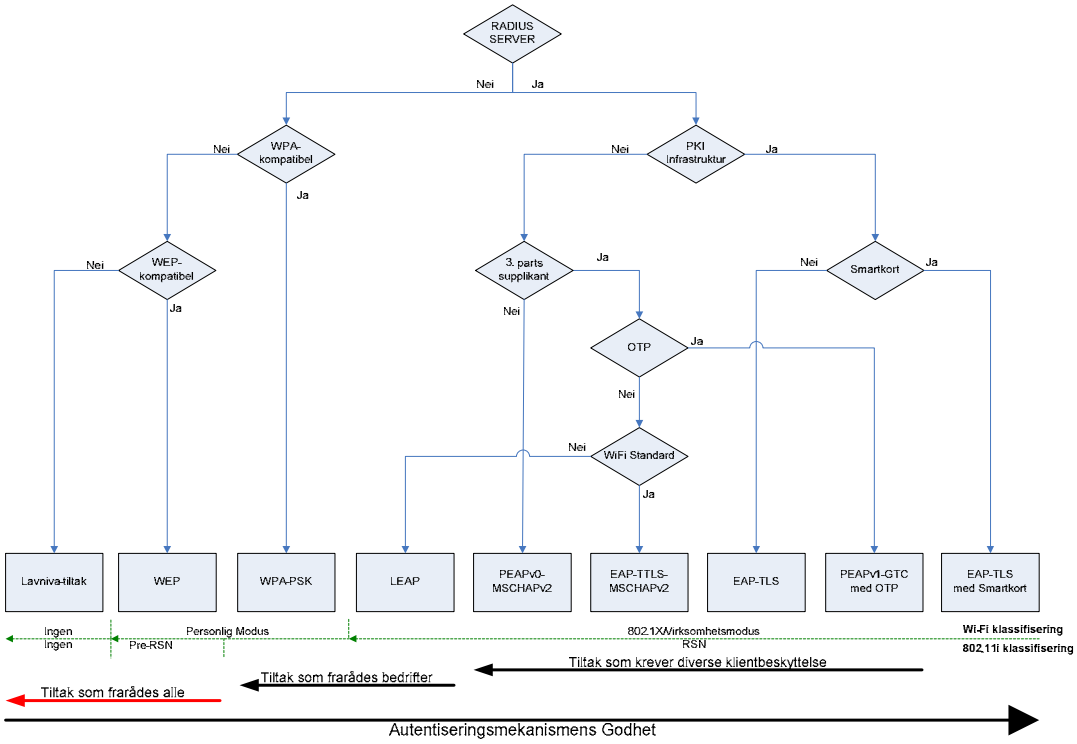
I vårt studie har vi konkludert med at den sikkerhetsmessige oppsiden ved en to-faktors autentiseringsløsninger er så avgjørende at OTP-løsningen basert på PEAP rangeres foran den protokollmessig mer robuste EAP-TLS løsningen, dersom smartkort ikke tas i bruk

Det er verdt å merke seg at rangeringslisten ikke tar hensyn til eventuelle administrative og merkantile kostnader knyttet til metoden. Flytdiagrammet på sin side kan, som nevnt, bidra til å synliggjøre noen av momentene som må tas i betraktning.

Rangeringslisten er som følger; beste først:

1. EAP-TLS med smartkortløsning
2. PEAPv1-GTC med enhet for engangspassord – One Time Password (OTP)
3. EAP-TLS
4. EAP-TTLS/MSCHAPv2
5. PEAPv0-MSCHAPv2
6. LEAP
7. WPA-PSK
8. WEP
9. Lavnivåtiltak/MAC-adressefilter

[10] Typisk en katalogtjeneste som Microsoft Active Directory, eller Novell eDirectory



Figur 2 Autentiseringsmekanismer i WLAN

X-aksen speiler rangeringslisten ovenfor og diagrammet kan leses slik; Dersom man av ulike årsaker ikke har mulighet for RADIUS-server i virksomheten kan man kun velge å benytte lavnivåtiltak eller løsninger som bygger delte nøkler, såkalt personlig modus. Ingen av disse metodene kan anbefales. Anskaffelse av en RADIUS server, muliggjør avansert og gode metoder for autentisering i et WLAN. Programvaren kan oftest tilegnes uten noen kostnad, enten som gratis programvare eller som en del av Microsoft Windows Serversystem. Dersom man allerede har en lisensiert versjon av Windows Server i organisasjonen, kan man uten ekstra kostnader benytte RADIUS-programvaren Internet Authentication Service (IAS)[11]. Det neste spørsmålet man må spørre seg er hvorvidt man har eller har mulighet for en full PKI-infrastruktur i virksomheten. Dersom en slik er på plass er EAP-TLS støttet. Dette er en god metode, og er i kombinasjon med smartkort rangert som den beste. Majoriteten av virksomheter har i dag ikke mulighet for PKI-infrastruktur. Dersom man har anledning til å anskaffe tredjeparts programvare[12] for WLAN-støtte (supplikant) på alle aktuelle enheter er det mulighet til å velge to-faktor autentisering basert på løsninger for engangspassord (OneTimePassword-OTP). OTP-løsninger har imidlertid også initielle- og vedlikeholdskostnader. Slike løsninger er relativt utbredt for

[11] Merk at ikke alle metodene i Figur 2 ovenfor er støttet på IAS. Imidlertid kan god RADIUS-programvare anskaffes relativt rimelig. Se Appendix ??? for en oversikt over tilgjengelig serverprogramvare og kompatibilitet.

[12] Merk: bærbart PC-utstyr fra produsenter som fokuserer på bedriftsmarkedet leveres ofte med egnet supplikant som tjene formålet. Eksempler på dette er HP som bundler Intel Proset Wireless og Lenovo (tidligere IBM) som tilbyr Thinkvantage Access Connections.

hjemmekontorløsninger, og vil kunne være et godt alternativ også for autentisering i det trådløse nettverket. Dersom man vil benytte samme brukernavn og passord som i virksomhetens trådbaserte brukerdatabase, så muliggjør metodene EAP-TTLS/MSCHAPv2 og PEAPv0/MSCHAPv2 dette. Metodene gjør det sågar mulig å tilrettelegge for fullstendig sømløs innlogging enten man er trådbunden eller –løs. I en moderne Windows infrastruktur vil PEAP-metoden være det opplagte valget da man klarer seg med den innebygde supplikanten i nyere Windows klientoperativsystemer samt den tidligere nevnte IAS for RADIUS støtte på serversiden. EAP-TTLS på sin side er svært orientert i retning programvare fra tidligere Funk Software, nå Juniper. Metoden som da gjenstår å kommentere er LEAP, som er en protokoll proprietær for Cisco Systems. I en tidligere tid hadde denne stor utbredelse, og fylte et behov i påvente av ratifisering av IEEE 802.11i. I 2003 ble det imidlertid klart at LEAP hadde alvorlige sårbarheter, og anbefales ikke lengre brukt. Det er heller ingen grunn til dette da Cisco de tidligere nevnte, mer robuste protokollene.

Figur 2 viser dessuten at dersom man velger en passord- eller sertifikatbaserte løsninger uten to-faktor autentisering, så kreves ekstra beskyttelse av de trådløse enhetene. Problemet består i det faktum at dersom enheten tapes vil uvedkommende enkelt kunne komme til autentiseringsdataene, enten det mellomlagrede passordet i MSCHAPv2-løsningene[13] eller klientsertifikatet i en EAP-TLS-basert løsning.

Dårlig konfigurerte PEAP- og TTLS-løsninger er sårbare for såkalte man-in-the-middle angrep. For å eliminere dette må klientene settes opp til å validere autentiseingsservers digitale sertifikat.

Vi har altså vist at CCMP i kombinasjon med en to-faktor autentiseringsløsning vil gi den teknisk sett mest robuste sikkerhetsløsningen med dagens tilgjengelige teknologi.

[13] Vi har ikke funnet det bevist at EAP-TTLS/MSCHAPv2 løsningen faktisk mellomlagrer passordet som en knekkbar hash på harddisk, men det vil uansett kunne være mulig til å finne spor av et slik når man tilbyr ”sømløs” login. Et Windows passord er i sin natur svært dårlig beskyttet når man har tilgang på den mellomlagrede hashen, som Windows login baserer seg på.

2. Tilsvarende arbeid

2.1.Teoristudiet

Det er gjort noe arbeid for å sammenligne godheten av sikringstiltak på WLAN. Det er en vesentlig del av kapittel 5 å korrelere funnene. Dette arbeidet er vist til i del 4-Teoristudium. Fellesnevneren for disse kildene er at de ikke har valgt de autentiseringsmetoder som er relevante for Wi-Fi sertifiserte produkter.

På tross av at det ikke har vært mulig å finne en rangering av godheten til metodene, er det imidlertid enighet om at WEP er et svært dårlig valg for konfidensialitet og integritet.

I nyere litteratur, med en viss tyngde er tendensen klar; nemlig at CCMP er beste metode for konfidensialitet og integritet. EAP-TLS er oftest metoden som anbefales for autentisering.

2.2. Empirisk undersøkelse

Når det gjelder den empiriske undersøkelsen, har det ikke vært mulig å finne sekundærdata som går i dybden på valg av sikkerhetsløsninger, og bakgrunnen for disse valgene. Som nevnt over, så har kartleggingsarbeid for det meste foregått som ustrukturerte wardriving-sesjoner, og i liten grad hatt fokus på hva virksomheter har valgt og hvorfor valget av sikringsmetode for WLAN har blitt slik det har blitt.

Kartleggingene foretatt gjennom wardriving har fokusert på å finne utbredelsen av krypterte og ukrypterte nett. Disse funnene har dårlig validitet ettersom de mest utbredte verktøyene for denne aktiviteten rapporterer nettverk sikret med moderne 802.1x autentisering som usikret.

Mørketallsundersøkelsen på sin side har utelatt autentisering i WLAN, og detaljerer eller årsaksforklarer heller ikke valget av krypteringsløsning. Den begrenser seg til å besvare spørsmålene om hvorvidt virksomhetene i det hele tatt har et WLAN, og hvorvidt dette er kryptert eller ikke.

Foruten å søke i tilgjengelig forskningsdatabaser, har det blitt rettet forespørsler til flere organisasjoner som kan tenkes å ha data på dette, for eksempel NorSis, Næringslivets sikkerhetsråd, IT-Sikkerhetsforum(ISF), Den Norske Dataforeningen, WAN.no, Abelia, Nettverket Trådløs Fremtid, HP, Aruba, Check Point og Symantec. Dette har ikke gitt noen uttelling.

3. Metode

I denne delen av redegjøres det for metoden som er valgt for å besvare forskningsspørsmålene. Forskningsspørsmål 1 vil besvares gjennom et kvalitativt teoristudium som vil gi et nødvendig teorigrunnlag for å kunne besvare spørsmål 2 og 3.

Spørsmålene 2 og 3 er praktiske problemstillinger som krever empiri. Det er viktig at den metode som velges er hensiktmessig for å kunne besvare forskningsspørsmålene. Disse danner grunnlaget for undersøkelsens kvalitative metodevalg.

Et eksplorerende design på teoristudiet, og et semistrukturert kvalitativt intervju med nøkkelpersoner i 5 norske virksomheter ga grunnlag for å kartlegge virksomheters valg og beveggrunnene for valgene.

3.1. Design

I litteraturen, typisk representert ved [FRA], skilles det mellom 3 typer design: Eksplorerende, beskrivende og kausale design. Eksplorerende design anvendes når problemstillingens karakter er uklar eller veldig grov. Det vil si at man står overfor et fenomen man ønsker å vite mer om, men har ingen klare formeninger hvordan dette kan analyseres. Beskrivende design anvendes ofte dersom forskningsspørsmålet skal beskrive en eller flere begreper eller variabler og sammenhengen mellom disse. Den tredje formen for design er kausale design og brukes i de tilfeller man ønsker å måle årsak og effektforhold, gjerne gjennom eksperimenter.

I forstudiet og den tidlige fasen av teoristudiet ble det studert metoder for sikring av trådløse nettverk, uten i utgangspunktet å ha noen klar formening om hva som kunne være aktuelle problemstillinger. En eksplorativ tilnærming. Det ble tidlig klart at det manglet en rangering av relevante sikkerhetsprotokoller for trådløse nettverk. Som en følge av dette har det blitt utarbeidet en slik rangering, og i tråd med forskningsspørsmålene har det blitt undersøkt i hvilken grad et lite utvalg norske virksomheters hadde sikkerhet som driver da de valgte sikkerhetsløsning, og i hvilken grad dette valget samsvarte med rangeringen som var utarbeidet.

3.2. Populasjon og utvalg

Et sentralt poeng er å bestemme en populasjon og utvalgsramme som er hensiktsmessig for å belyse de aktuelle forskningsspørsmålene. Det er viktig at populasjonen har en slik sammensetning at populasjonsmedlemmene har en lik oppfatning av begrepene som anvendes i undersøkelsen.

Det er imidlertid viktig å poengtere at med et såpass begrenset utvalg er det ingen mulighet til å trekke statistiske konklusjoner, noe som heller ikke er målet med dette studiet av trådløse nettverk. Utvalget er i sin helhet gjort med tanke på å belyse problemstillingen på en best mulig måte innenfor rammen av studiens omfang

Kravet som ble stilt til utvalget av virksomheter var at de skulle ha et trådløst nettverk i drift, og være tilgjengelige for å dele informasjonen. I tillegg var det et vesentlig poeng å finne virksomheter hvor jeg ikke hadde kunnskap om eksisterende

infrastruktur og årsak til valg av løsning. Det ville i så fall vært fristende å velge caser som underbygge de forventede funn.

Av ressurshensyn er det valgt virksomheter hvor forfatteren har kontakter. Gjennom disse har det blitt valgt ut nøkkelpersonell som antas å være opptatt av problemstillingen og positive til å utlevere denne type informasjon, men allikevel faller inn under kategorien over, nemlig at jeg ikke har kunnskap om infrastrukturen på forhånd. Dette har sin bakgrunn i begrensede rammebetingelser, samt at det antas å være enkelt å få tilgjengeliggjort ønsket informasjon.

I litteraturen [SEL] omtales dette som ett av tre valg innen for Ikke-sannsynlighetsutvalg; nemlig et bekvemmelighetsutvalg. Overrepresentasjon er da typisk, og i dette tilfellet vil vi være overrepresentert med at samtlige i en eller annen form er i nettverket til forfatteren. Dette er en utvalgsform som i sin natur kan, og sannsynligvis vil, gi systematiske skjevheter.

Dette vil vanligvis kunne virke inn på validiteten i en kvantitativ undersøkelse, men antas ikke å ha noen konsekvens her ettersom vi ikke ønsker å trekke noen statistiske konklusjoner. Vi ønsker kun å se på valg av sikkerhetsprotokoller, og beveggrunnen for dette valget i en liten gruppe for å se om dette er samsvarende med rangeringen som er laget.

Det er valgt ut 5 virksomheter fra både offentlig og privat sektor. Virksomhetene fra privat sektor er børsnoterte selskaper som forvalter og beskytter enorme verdier både i form av bedriftsintern informasjon og økonomi- og kundedata. Virksomhetene fra offentlig sektor er skoler som er blant de største i landet hva elev- og ansatt tall angår, og forvalter til dels også sensitive data. Alle har til felles at de har profesjonelle IT-organisasjoner med egne ansvarlige for fagområdene nettverk og sikkerhet. De forvalter selv en stor del av den intellektuelle kapitalen på området og samtlige har langt over 1 000 brukere.

Etter at intervjuene var gjennomført pekte resultatene entydig i retning av at valgene som i sin tid ble gjort, var basert på anbefalinger fra leverandører. Vi valgte derfor uformelt å kontakte 3 leverandører[14] for å finne ut hvilke løsninger de anbefaler i dag, og hvorfor. De ble valgt ut 2 ledende WLAN-produsenter med egne tekniske konsulentavdelinger, og ett anerkjent konsulentselskap som yter konsulentbistand, samt designer og leverer løsninger basert på markedsledende merkevarer. Det er ikke gitt at disse leverandørene har gitt anbefalinger til våre intervjuobjekter.

3.3. Datainnsamling

Den empiriske undersøkelsen baserer seg på innhenting av primærdata fra intervjuobjekter i sentrale stillinger i virksomheter som har blitt valgt ut. Et like detaljert studium ser ikke ut til å ha blitt gjort tidligere. På tross av at teoristudiet

[14] Det uavhengige forsknings- og rådgivningsfirmaet Gartner Group har de siste 2 årene rangert to av disse som ”visjonære ledere” med høy leveringsevne i sin ”Magic Quadrant”. Den tredje er blant”utfordrerne” med høyest leveringsevne.

innenfor området autentisering konkluderer annerledes enn tilgjengelig sekundærdata, så baserer den seg på, og støtter seg til allerede kjente funn og drøftinger, men trekker inn sentrale momenter fra andre deler av litteraturen om informasjonssikkerhet. Dette er momenter har en sentral plass både i "beste praksis" og i litteraturen om autentisering, i litteraturen omkring av autentisering i trådløse nettverket er disse mekanismene oppsiktsvekkende fraværende.

3.3.1. Teoristudium

Teoristudiet har tatt sitt utgangspunkt i mange grundige litteratursøk i tilgjengelig anerkjent litteratur, og søk i databaser som er tilgjengelige fra Høgskolen i Gjøvik. Google Scholar har koblinger til mange anerkjente vitenskapelige databaser, og viste seg som en overraskende positiv og seriøs ny tjeneste. Ulempen er at mange av disse er betalingstjenester. Bruk av Høgskolens proxytjenere muliggjorde søk også når man arbeidet fra en annen lokasjon, noe som var en nødvendighet her.

Eksempler på databaser som har blitt brukt gjennom Høgskolens proxytjener er IEEEexplore, ACM, Citeseer, ISI Web of Science, Springerlink og Firstsearch. Flere av databasene tilbyr også siteringssøk, noe som har vært brukt for å få en pekepinn om kildens seriøsitet, og hvor kjent den er for fagmiljøet.

Et "ITPro-abonnement" på books24x7.com har også vært ekstremt verdifullt. Nettstedet tilbyr ultimo oktober 2007 6456 IT-bøker med totalt 3 147 266 sider fra anerkjente forlag som for eksempel McGraw-Hill, Artech House, Syngress Publishing og John Wiley & Sons

3.3.2. Empirisk undersøkelse

Formålet med den kvalitative metoden er ikke å gjøre generaliseringer, men snarere å gjøre en undersøkelse i forhold til forskningsspørsmålene og antakelsene vi har.

Intervjuformen er spesielt egnet når man ønsker å undersøke hvordan mennesker forstår sin egen verden[KVA]

Dersom antagelsen om at man ikke alltid velger den sikreste løsningen er korrekt, vil avdekking av et slikt funn lettest gjøres gjennom en kvalitativ metode, som intervjuet er. Bakenforliggende årsak til valget kan antakelig forstås enklere når man forstår intervjuobjektets verden, og får mulighet til å stille oppfølgingsspørsmål.

Det har blitt valgt et semistrukturert intervju, hvor intervjuer støtter seg til utarbeidet intervjuguide uten at denne er noen fastsatt mal som vi må forhold oss 100 % til.

Intervjuguiden ble pre-testet og viste seg å fungere hensiktsmessig, med et par tilføyelser og endring av rekkefølgen på et par spørsmål. Intervjuobjektene i pre-test fikk også en kopi av intervjuguiden, noe man valgte å ikke distribuere på forhånd ved senere intervju. Det viste seg i pre-test at fokus lett ble trukket mot fagterminologien og skisse av potensielle svar i intervjuguiden, fremfor å resonere rundt spørsmålene.

Intervjuobjektet vil dessuten føle seg friere til å svare åpent på spørsmålene dersom han ikke har en rekke forslag med svar som notert i guiden.

Resultat av pre-test var altså verdifull i den forstand at innholdet ble noe justert, samt en visshet om at et semistrukturert intervju er en egnet metode, ettersom det fremkom langt flere relevant opplysninger enn vi ville fått ved et spørreskjema som ikke gir mulighet for utdypninger og oppfølgingsspørsmål.

3.4. Analyse av data

Vi har gjennom datamaterialet fått belyst de ønskede sider av den overordnede problemformuleringen. Teoristudiet har satt oss i stand til å lage en rangering av godhetene av tilgjengelige metoder, således er forskningsspørsmål 1 besvart. Gjennom intervjuene har vi samlet data som muliggjorde å besvare forskningsspørsmål 2 og 3, samt belyse de antakelsene vi hadde da arbeidet ble påbegynt. Dette er utdypet i kapittel 6.

Når det gjelder betraktninger omkring validitet og reliabilitet finner vi det mest hensiktsmessig å belyse dette under ett:

Som vist i kapittel 3.3.1 har det blitt brukt anerkjente kilder av sekundærdata for å belyse problemstillingen. Som kommentert i 1.1 Problembeskrivelse, er selv den tradisjonelt mest anerkjente litteraturen på området av svært varierende kvalitet, og det er dette er en av hovedårsakene til at teoristudiet har vært nødvendig å gjennomføre. Som en konsekvens av dette har det i mange sammenhenger vært nødvendig å innhente data fra de mest autoritative kildene på området, nemlig IEEE standardene og RFC[15]-ene fra IETF[16]. Når funnene i litteraturen og forskningsartiklene har blitt kvalitetssikret og korrelert mot de autoritative kildene innenfor vår kontekst mener vi at resultatet i form av teoristudiet i denne rapporten er reliabelt.

I 4.4.1 og 4.4.2 ser vi på henholdsvis validitet i forhold til intervjuene som var nødvendige for å besvare forskningsspørsmål 2 og 3.

Validitet, også kalt gyldighet, vil i vår kontekst dreie seg om vi måler det vi tror vi måler. Det vil si hvorvidt forskningsspørsmålene blir besvart. Sentralt for å kunne besvare forskningsspørsmål 2 og 3 er kravet til utvalgets gyldighet i forhold til problemstillingen. For å kunne belyse disse på en hensiktsmessig måte har det vært nødvendig å intervjue de personene i virksomhetene som har dybdekunnskap om valgene som har vært gjort. Dette har vært virksomhetenes nettverks- og sikkerhetsanvarlige.

Forskerens ståsted, faglige interesser og personlige erfaringer avgjør hvilken problemstilling som er den aktuelle, hvilket perspektiv som skal velges, hvilke metoder og utvalg som er relevante, hvilke resultater som besvarer de viktigste spørsmålene og hvordan konklusjonene skal vektlegges og formidles. Spørsmålet er ikke hvorvidt forskeren påvirker prosessen, men hvordan. Forskeren/intervjueren ønsker i størst mulig grad å være en objektiv uhildet fagperson, men ettersom dette er umulig er det nødvendig at han er seg bevisst nettopp denne problemstillingen; nemlig at forskeren påvirker prosessen ref [MALT] I dette ligger en del teknikker i forhold til kravet å

[15] RFC-Request for Comments. Betegnelse på dokumentserie som beskriver IETFs standarder.

[16] IETF – Internet Engineering Task Force

gjennomføre intervjusituasjonen. Som en følge av dette er det blant annet avgjørende å ikke avsløre egne holdninger og funn som jeg har gjort i teoristudiet.

Uavhengig av funnene som er gjort i denne oppgaven er det opplagt at funnene ikke nødvendigvis vil være de sammenfallende med funn i andre virksomheter. Til det er fagområdet alt for omfattende og mangefasettert, med for lang og spesiell historie. Ulike virksomheter vil dessuten ha ulik infrastruktur og ulike krav til sikkerhet.
I studier av denne typen handler reliabilitet, ofte kalt pålitelighet, i hovedsak om hvorvidt intervjuobjektene snakker sant. Årsaker til at objektene kan velge å tilsløre sannheten, eller med overlegg å snakke usant vil kunne være flere. Eksempler på dette vil være at dersom en dårlig metode er valgt vil vedkommende kunne ønske å stille seg selv eller virksomheten i et bedre lys, for eksempel ved ansvarsfraskrivelse eller ved å gi feilaktige opplysninger. I stor grad har dette problemet vært eliminert ved at intervjuer ved selvsyn fikk se på konfigurasjon. Hvorvidt ansvaret for et dårlig valg ligger hos intervjuobjektets selv eller noen andre er underordnet i denne sammenhengen. Alle virksomhetene og intervjuobjektene er dessuten anonymisert.

Intervjuobjektene var utelukkende nettverks- og sikkerhetsansvarlige i virksomhetene de arbeidet. Flere av dem hadde aktivt deltatt i valg og konfigurasjon av systemet. Dette i seg selv vil, rent objektivt sett kunne være en medvirkende årsak til at reliabiliteten vil være dårligere, men intervjuers innsyn i konfigurasjon eliminerer altså langt på vei dette. Alternativet ville være å velge personer som ikke hadde hatt noe med valg eller konfigurasjon å gjøre. Dette ville imidlertid gått ut over validiteten.

4. Teoristudium

Det har blitt hevdet at sikkerhetens verste fiende er kompleksitet:

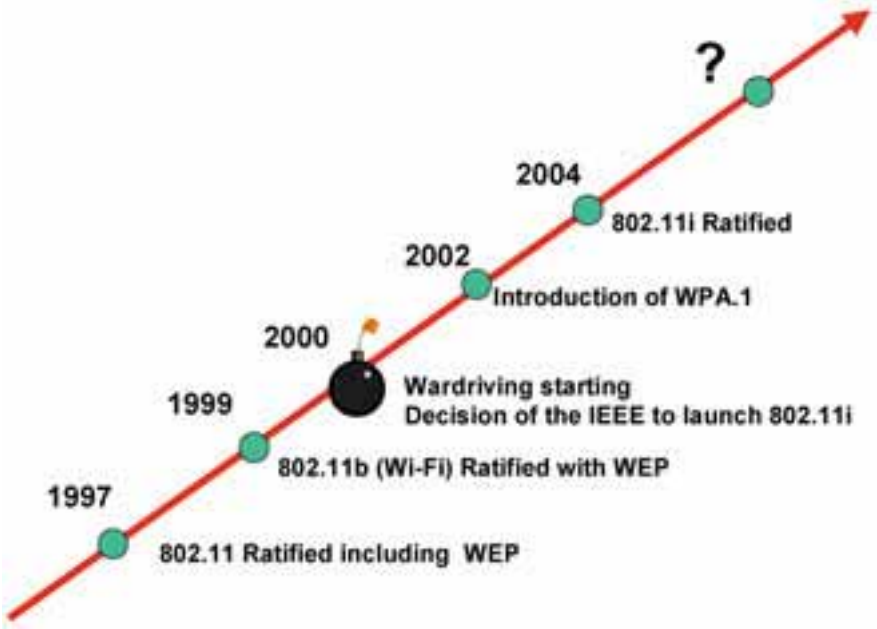
The future of digital systems is complexity, and complexity is the worst enemy of security[SCH]

"Complexity is the enemy of security" [SKO]

Foruten at sentrale aktører i miljøet, som over uttaler dette, er dette åpenbart for alle som har forsøkt å forstå sikkerheten rundt protokollene og de tekniske sikkerhetsmekanismene etter 802.11 standardene at dette er svært komplekst område.

Det er imidlertid mulig å minimere en av faktorene som gjør utsagnet over til en sannhet. Kunnskap om protokollenes oppbygging og trusselbildet knyttet til disse vil være nøkkelen til å velge en trådløs løsning som er sikrest mulig. Dette er årsaken til at temaet krever en relativt grundig behandling på teoretisk nivå.

4.1. Utvikling av sikkerhetsløsninger for WLAN



Figur 3 Utvikling av sikkerhetsløsninger[KHA]

På tidsaksen i Figur 3 ser vi utviklingen av sikkerhetsløsninger som har vært tilgjengelig for WLAN etter 1997. Behovet for utvikling av mer robuste løsninger ble åpenbart etter at såkalt wardriving begynte å bli utbredt i 2000.

4.2. WLAN-Fordeler

Trådløse nett har mange fordeler, både på generell basis og sammenlignet med tradisjonelle trådbaserte nett [NIST800-48]. De mest fremtredende fordelene defineres som:

Mobilitet

Brukerne får tilgang til internett, filer og nettverksressurser uten å være fysisk tilknyttet nettverket med tradisjonelle kabler. Dette vil gi en økt grad av frihet ved bruk av nettverksressurser.

Rask installasjon og lav pris

Ingen behov for å trekke kabler. Denne jobb er tradisjonelt kostbar og tidkrevende.

Fleksibilitet

Trådløse nett kan raskt og enkelt installeres for ad-hoc formål, for ulike behov og arrangementer som konferanser og møter.

Skalerbarhet

Topologien gir rom for enkelt å skalere fra små peer-to-peer nettverk til større virksomhetsnettverk for å muliggjøre nettvandring[17] over et stort område

4.3. Informasjonssikkerhet og WLAN

I september 2007 ble det klart at gjennom et brudd på sikkerheten i WEP hos den amerikanske kjeden TJX hadde datakriminelle skaffet seg tilgang til kundesystemet, og over en periode på sju måneder ubemerket fått tilgang til 80 GB data; herunder i underkant av 100 millioner kundekontoer

Av opplysningene man med sikkerhet vet er på avveie er data som personnavn, trygdenummer[18], bankkontoer og kreditt- og betalingskortinformasjon. Disse dataene i seg selv, eller i kombinasjon, muliggjør grunnlaget for en av vår tids mest fryktede problemstillinger: Identititetstyveri.

I rene økonomiske utgifter for TJX, unntatt utfallet av evt søksmål fra myndigheter, kunder og kredittkortleverandører, estimerer det anerkjente Forrester Research at denne episoden hos TJX kan beløpet seg opp mot summer i størrelsesorden 1 milliard dollar over en 5 årsperiode. Sikkerhetsoppgraderingene alene anslås til å beløpe seg tilover 100 millioner dollar. Kortleverandørene lider fremdeles store tap som følge av denne episoden, og Visa anslår at frem til nå har deres kort blitt misbrukt i 13 land, med beløp i størrelsesorden opp mot 83 millioner dollar [WALL],[BUS]

Alle trusler som eksisterer i et kablet nett vil også finnes i et WLAN, men sistnevnte er i ennå større grad sårbare for angrep vi tradisjonelt har forbundet med kablede nett som Man-in-the-middle-attacks, maskering[19] og session hijacking. Det har blitt hevdet at WLAN-risikoer er ekvivalent med summen av tradisjonelle risikoer pluss de nye introdusert i WLAN. Total beskyttelse mot aktive og passive angrep anses umulig i et trådløst dersom signalene er innenfor rekkevidde [NIST 800-48]

Angrep mot WLAN-sikkerheten har tidligere vært synonymt med mindre alvorlige handlinger som utføres av nysgjerrige amatører. En rapport utarbeidet av Nasjonal Sikkerhetsmyndighet (NSM) peker på at dette har endret seg radikalt de siste par

[17] Engelsk: “Roaming”

[18] Amerikansk: ”Social security number”

[19] Eng: spoofing

årene. Angriper kan ha ulike motiver, men tendensen er at omfanget av politisk- og økonomisk motiverte angrep er omfattende og stadig økende. Det er dessuten symptomatisk at handlingene i stadig større grad nå utføres av fagspesialister, som også har tilbudt sine tjenester for organiserte grupperinger som utøver økonomisk motivert kriminalitet. Skal vi tro undersøkelsen vil denne trenden fortsette og trusselaktører trenger ikke selv å bygge datakompetanse for å utgjøre en reell trussel. Isteden kan trusselaktører kjøpe seg nødvendig hjelp og kompetanse [NSM].

4.3.1. Angrep på informasjonssikkerhet

En formell definisjon av informasjonssikkerhet finnes i [DAL].

Informasjonssikkerhet defineres som
Beskyttelse mot brudd på konfidensialitet, integritet og tilgjengelighet for den informasjonen som behandles av systemet og systemet i seg selv

Definisjonen krever utledning av sikkerhetstjenestene i definisjonen

Konfidensialitet

Sikkerhet for at kun autoriserte personer får tilgang til følsom eller gradert informasjon, og at det på forhånd er foretatt en gyldig identifisering og autentisering av personen

Integritet

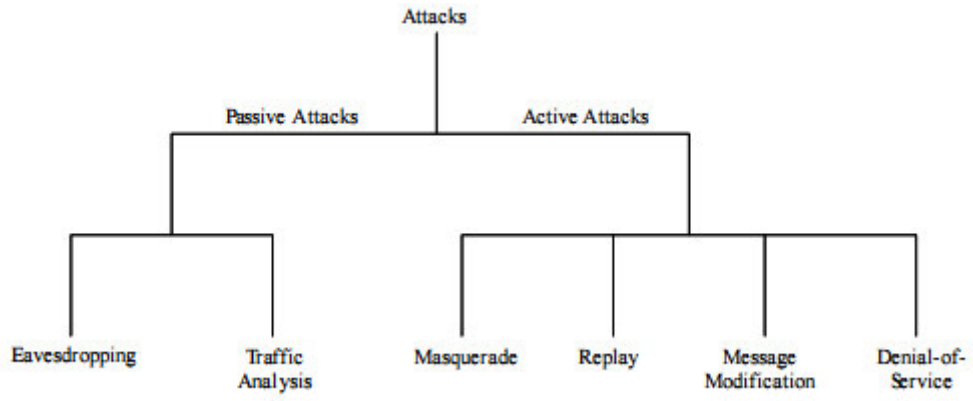
Sikkerhet for at informasjonen og informasjonsbehandlingen er fullstendig, nøyaktig og gyldig, og et resultat av kontrollerte aktiviteter

Tilgjengelighet

Sikkerhet for at en tjeneste oppfyller bestemte krav til stabilitet, slik at aktuell informasjon er tilgjengelig ved behov.

I tillegg til dette definerer standarden X.800 [X.800]og flere autoriteter autentisering som en av sikkerhetstjenestene. Sentralt i vår videre drøfting vil være konfidensialitet, integritet og autentisering.

X.800 definerer følgende generelle taksonomi for angrep mot de definerte egenskapene.



Figur 4 Typer angrep [STA]

4.3.2. Passive angrep

Passive angrep defineres som angrep som bryter konfidensialitet men ikke integritet. Slike angrep kan realiseres som avlytting eller trafikkanalyse.

Avlytting

Angriper avlytter overføringer for å få kjennskap til innholdet. Brudd på konfidensialitet.

Trafikkanalyse

Angriper får tilgang til overføringer for å analysere hvor trafikken flyter. Brudd på konfidensialitet

4.3.3. Aktive angrep

Aktive angrep defineres som et angrep hvor angriper deltar med aktive handlinger, som i seg selv, eller med utgangspunkt i disse har til hensikt å bryte integritet eller tilgjengelighet.

Maskering

Angriper utgir seg for å være en autorisert bruker for å få uautorisert tilgang til ressurser. Brukes gjerne i kombinasjon med andre angrep som har til hensikt å skaffe seg uautorisert tilgang. Aktiviteten har til hensikt å bryte konfidensialitet og integritet.

Replay

Angriper avlytter først trafikk gjennom et passivt angrep, utgir seg for å være en autorisert bruker, gjennom maskering, og retransmitterer dataene som denne. Dette vil gi brudd på opprinnelsesintegritet.

Endring av melding

Angriper endrer en melding under overføring gjennom å slette, legge til, eller endre denne. Brudd på integritetskravet.

Tjenestenekt

Angriper hindrer legitime brukere å nå systemene. Tjenestenekt (DoS - Denial of Service) er en angrepsmetodikk som har til hensikt å gjøre autoriserte tjenester utilgjengelig for legitime brukere. I det trådløse nettverket kan et slikt angrep komme fra hvor som helst, pga. fritt luftrom.

Men DoS trenger ikke å komme fra en ondsinnet hacker. Siden Wi-Fi opererer på det uregulerte 2.4GHz radiofrekvensen som er også brukt av blåtann-enheter, mikrobølgeovner, babyovervåkere og trådløse telefoner, kan disse skape forstyrring i luftrommet og dermed føre til tjenestenekt i WLAN-et.
Tjenestenekt, fører altså til brudd på tilgjengelighetskravet og vil ikke være noe tema videre, jf. kapittel 1.2

4.3.4. Andre utfordringer

Det ligger i sakens natur at trådløse nettverkstilgang vil gi tilgang til virksomhetens trådbaserte nettverksressurser dersom den skal ha virkelig verdi. Dette medfører en rekke nye trusler. Ikke alle moderne angrep passer inn i modellen [X.800], [STA]. For å vise omfanget av trusselbildet vil vi vise til noen andre utfordringer som ikke uten videre passer inn i modellen. Disse er hovedsakelig basert på arbeidet til [EDN], [EAR] og [VLA]. Listen er ikke uttømmende.

Oppheving av perimeterne

Tradisjonell skallsikring som adgangskontroll og alarm, og brannvegger som perimetersikring mot eksterne nettverk er utilstrekkelig for å beskytte infrastrukturen når man med et trådløst nettverk distribuerer nettverksressursene. Begrensning av fysisk tilgang er altså ikke lengre mulig[20]. Har man tilgang til radiosignalene så har man potensiell tilgang til nettverket, fysisk utenfor det kablede nettverket, men likevel på innsiden perimetersikringen.

Falske aksesspunkter og tilfeldige forbindelser

Ved å konfigurere en arbeidsstasjon om til et aksesspunkt, eller sette opp falske aksesspunkter[21] kan det utføres flere sofistikerte angrep. Falske aksesspunkter, er sentralt for å kunne realisere et man-in-the-middle angrep, noe som kan utnyttes selv i moderne løsninger etter 802.11i standarden. Mer om dette i kapittel 4.14.8. Problemet med såkalte tilfeldige forbindelser oppstår når et nærliggende aksesspunkt, tilbyr sine tjenester til andre brukere enn tilsiktet. Problemet her er todelt: Eksponering av arbeidsstasjonen og eksponering av andre ressurser som er knyttet til arbeidsstasjonen. Dette vil gjennom andre svakheter i systemet kunne utnyttes til å skaffe tilgang til nettverkets ressurser, eller til å installere bakdører, eller spre ondsinnet programvare som virus, trojanere – eller på andre måter bryte systemets konfidensialitet, integritet eller tilgjengelighet.

Split tunneling

Det eksisterer også en reell trussel i at en legitim arbeidsstasjon på et fremmed/fiendtlig WLAN kan kobles sammen med et virksomhetsnettverk, enten fysisk med en kabel i virksomheten trådbaserte nettverk eller virtuelt for eksempel over internett via en VPN-tunnel. Arbeidsstasjonen vil da ha ett grensesnitt[22] mot det fiendtlige nettet og ett grensesnitt mot virksomhetsnettverket, og kunne fungere som en bro eller ruter mellom disse. Man har i praksis etablert en bakdør inn i nettverket. Fenomenet, som ofte kalles ofte ”split tunneling”, har lenge vært en del av trusselbildet i forhold til VPN løsninger, og mange virksomheter legger ned betydelig arbeid for å unngå dette.

Hotspots

Flere virksomheter tilbyr egne WLAN-soner for ren internett-aksess, såkalte Hotspots. Disse er infrastrukturmessig ofte plassert utenfor brannvegger eller i egne soner hvor man mener at et lavt sikkerhetsnivå er akseptabelt. Tilgang til et slikt nett for en ondsinnet vil kunne være et utgangspunkt for å drive ondsinnede aktiviteter bak en IP-adresse som tilhører virksomheten. Dette vil potensielt kunne føre til tap av renommé for virksomheten dersom aktiviteten blir kjent. Dels fordi virksomheten kan ha tilbudt tjenester som har blitt utnyttet, og formelt står ansvarlig for adressene dette skjedde fra, dels fordi det vil bli kjent at virksomheten har vært utsatt for et sikkerhetsbrudd.

---

[20] Det vil være mulig å begrense radiosignalene ved bruk av såkalte Faraday bur eller – skjold, men dette er både kostbart og lite aktuelt annet i høysikkerhetsmiljøer. I slike miljøer vil det antakelig heller ikke anses som sikkerhetsmessig forsvarlig å distribuere nettverket trådløst heller innenfor skjoldets grenser.

[21] Eng: Rogue accesspoint

[22] Eng: Interface, på norsk også kalt “bein” eller bare nettverkskort

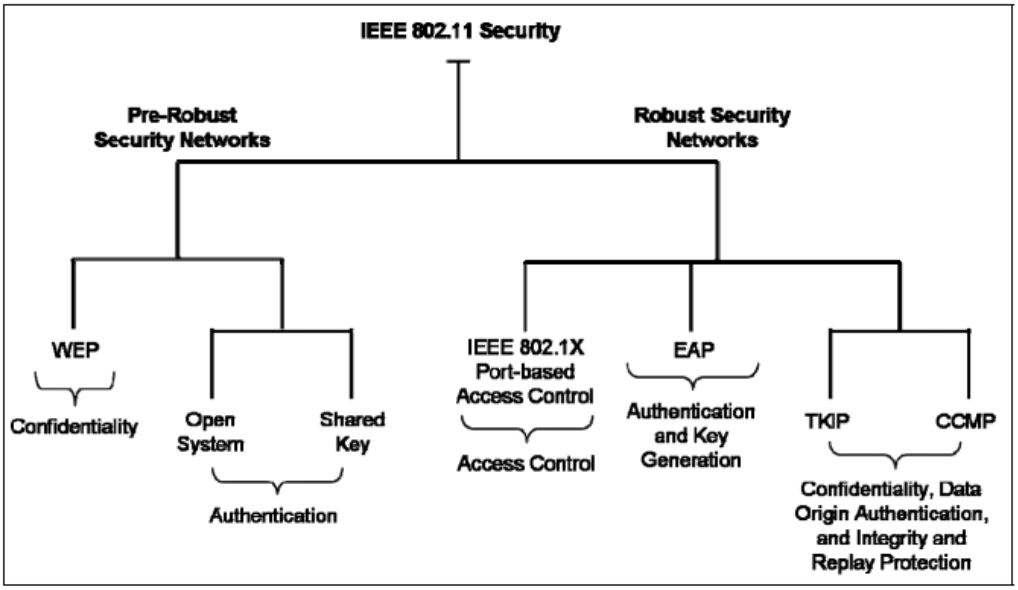
Problemstillingene er relevante og viktige, men utover falske aksesspunkter er videre drøfting utenfor denne oppgavens rammer. Det henvises til litteraturlisten for mer informasjon.

4.4. Oversikt over sikkerhetsløsninger

Vi vil i det etterfølgende se på tekniske sikkerhetsløsninger trådløse nett. I dette kapittelet ser vi overordnet på sikkerhetsløsningene, for i senere kapitler å detaljere disse.

Denne oppgaven drøfter sikkerhetsmetoder etter 802.11 standarden. Denne standarden er utviklet og vedlikeholdes av The Institute of Electrical and Electronics Engineers, Inc. (IEEE). IEEE er en non-profit organisasjon som samler fagfolk innenfor elektroteknikk, og har 365 000 medlemmer, herav 842 norske, i over 150 land.

IEEE er sentral innenfor utvikling og vedlikehold av standarder for datanettverk. Vi har fokus på 802.11, men IEEE har også bidratt med blant annet de facto standarden for kablede nettverk, nemlig IEEE 802.3, bedre kjent som ethernet.



Figur 5[NIST800-97]

Sikkerhetsløsninger for trådløse nett ble første gang ratifisert i 802.11-standarden i 1997, og senere revidert i 1999 [802.11-1999]. Mekanismen som blir brukt for å tilby sikkerhet i denne standarden er Wired Equivalent Privacy (WEP). Metoden benyttes for så vel konfidensialitet og integritet. Selv om det er et krav i standarden at implementasjoner skal tilby Open System, ofte kalt ”null-autentisering”, dvs ingen autentisering, [23] så åpner den for bruk av WEP også til dette formålet. Sikkerheten baserer seg på en nøkkel, WEP-nøkkel, som deles mellom alle enheter i det trådløse nettverket. Metoden kalles Shared Key.

[23] utover MAC-adresse, som ikke kan kalles autentisering etter vår definisjon

Rundt tusenårsskiftet ble det klart at WEP hadde store svakheter og mangler. Som en konsekvens av dette ble en ny standard utarbeidet. Denne ble ratifisert av IEEE i 2004 [802.11i]. Standarden beskriver to typer sikkerhetsregimer: Den introduserer begrepet Robust Security Networks (RSN), som tilbyr sikkerhet for konfidensialitet og integritet gjennom to ny sikkerhetsprotokoller; TKIP og CCMP. TKIP baserer seg på den sårbare WEP-protokollen, men eliminerer alle kjente sårbarheter i denne. CCMP på den annen side er basert på AES[24] for konfidensialitet og CBC-MAC for integritet. TKIP og CCMP omtales ofte som henholdsvis Wi-Fi Protected Access (WPA) og WPA2. I praksis brukes begrepene 802.11i, WPA2 og RSN om hverandre. Det er også en allmenn oppfatning at WPA er ekvivalent med bruk av TKIP under 802.11i standard.

WEP er også beskrevet i [802.11i], men omtales da som Transient Security Network (TSN), eller Pre-Robust Security Networks (Pre RSN). Som det fremgår av navnet er metoden ikke anbefalt og det spesifiseres at dersom denne må brukes, så bør dette bare skje i en overgangsfase under migrering til RSN.

Standarden overlater i stor grad spørsmålet om autentisering i et RSN til andre standarder, men spesifiserer at den overordnet kan gjøres på 2 måter

Enten gjennom bruk av forhåndsdelte nøkler mellom alle enheter i RSN. For brukerne oppleves dette ekvivalent med bruken av WEP i et TSN, men sikkerheten er i praksis mye bedre. Metoden omtales ofte som WPA-PSK, hvor PSK står for preshared keys, og anbefales bare brukt dersom man av ulike årsaker ikke har mulighet til alternativet. Det andre og mer robuste alternativet som anbefales brukt i et RSN, er 802.1X-infrastruktur for aksesskontroll og EAP for autentisering og nøkkelhåndtering. Wi-Fi alliance omtaler disse to metodene for autentisering som henholdsvis WPA Personal Mode og WPA Enterprise Mode[25]. Dette diskuteres detaljert i kapittel4.13.

4.5. WLAN arkitektur

Essensielle komponenter i en WLAN-arkitektur er STA og AP, som vi definerer slik; avledet av [802.11i]:
STA – Formelt i hht 802.11i: Enhver enhet med et trådløst nettverkskort som interfacer mot det trådløse nettverket. I denne rapporten brukes STA som betegnelse på trådløse enhter som ikke er aksesspunkter. Typisk en bærbar PC.
AP – En node på nettverket som tilbyr tilgang til et nettverk via radiosignaler. Er ofte en bro eller en ruter inn til en kablet infrastruktur

Et WLAN kan operere i 2 ulike modi.
Modus 1
Infrastructure Basic Service Set (BSS) hvor man har et AP. Flere BSS kan til sammen forme et Extended Service Set (ESS) gitt at de har samme SSID. Kalles heretter infrastruktur modus.

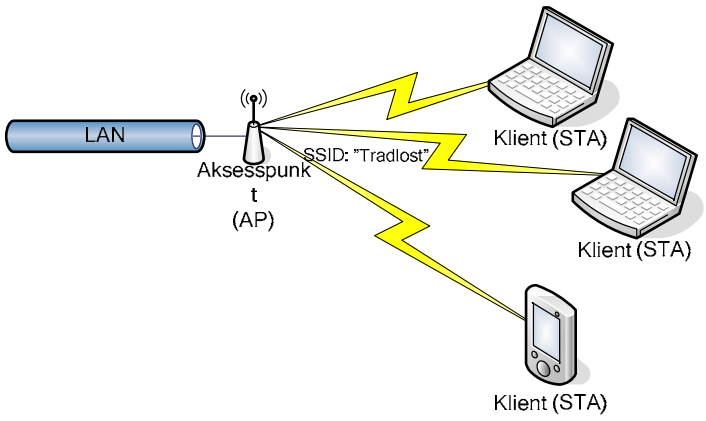
Modus 2
Ad-hoc også kalt Independent Basic Service Set (IBSS)

[24] AES – Advanced Encryption Standard

[25] I denne rapporten omtales de også som henholdsvis Personlig Modus og Virksomhetsmodus

4.5.1. Infrastructure

Et WLAN i infrastrukturmodus består av ett eller flere AP og en eller flere trådløse enheter, typisk bærbare PC-er eller håndholdte enheter (STA) med trådløst nettverkskort. AP består av en radiosender/-mottaker (tranceiver) som klientadapterne kobler seg til og får derfra tilgang til det kablede nettet via en kabel i aksesspunktet. Denne metoden kalles punkt-til-multipunkt, eller infrastructure modus, og er som oftest den metoden man tenker på når man snakker WLAN. Dette er vist i Figur 6 Infrastruktur Modus



Figur 6 Infrastruktur Modus

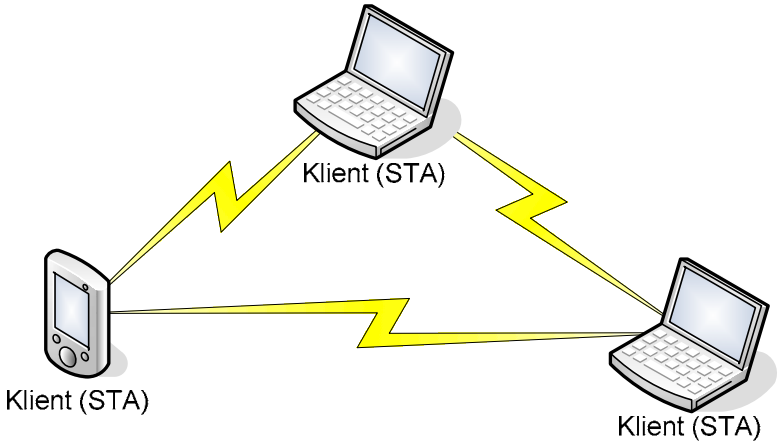
802.11-standarden omtaler infrastrukturmodus som BSS, eller en samling BSS for et ESS. Større virksomheter vil naturlig ha et eller flere ESS, ofte på tvers av landegrenser. Imidlertid er dette lite innarbeidede begreper, slik at vi konsekvent bruker infrastruktur modus som benevnelse enten det er et BSS eller et ESS.

STA kommuniserer med hverandre ved å gå igjennom et AP. AP fungerer som en HUB for kommunikasjonen. I tillegg vil et AP i de fleste sammenhenger gi tilgang til en virksomhets kablede nettverksressurser. Dette tas som en forutsetning i det videre arbeidet.

4.5.2. Ad-hoc

Ettersom alle klientadapterne inneholder både sender og mottaker er det også mulig å etablere direkte kontakt mellom klientadapterne uten å gå via et aksesspunkt. Dette kalles gjerne et mange-til-mange-nettverk, eller et ad-hoc-nettverk evt IBSS i [802.11i]. I en slik topologi, eller en mix mellom ad-hoc og infrastruktur modus kan evt. en av klientene fungere som en bro mellom ad-hoc-nettet og et annet nett, kablet eller et trådløst nettverk i infrastruktur modus. Dette er en lite ønskelig situasjon som man må være oppmerksom på i sikkerhetsarbeidet.

Denne modus er imidlertid i liten grad berørt i oppgaven, jf. avgrensninger i innledende kapittel 1.3



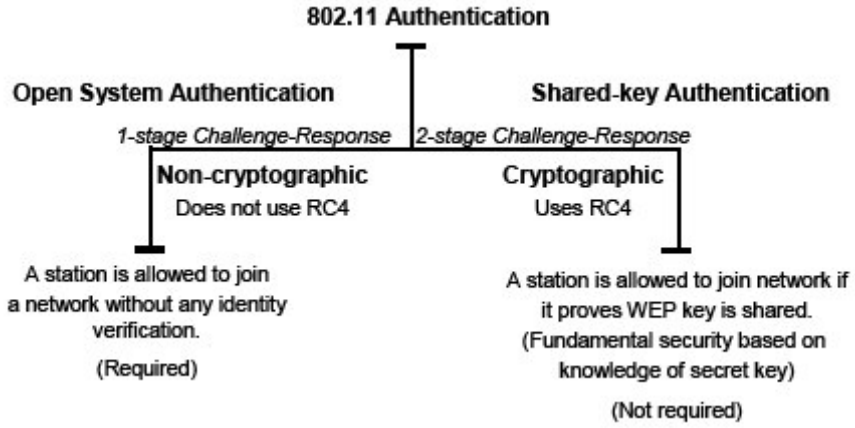
Figur 7 Ad-hoc modus

4.6. Pre-RSN sikkerhet/WEP

WEP er den opprinnelige metoden for å beskytte det trådløse nettverket etter standarden [802.11-1999]. WEP er også en opsjon i den nyere standarden [802.11i]. I beskrivelsen i dette kapittelet vil fokus være etter [802.11-1999].

4.6.1. Autentisering i WEP

802.11 standarden beskriver to typer autentisering; open system og shared key autentisering.



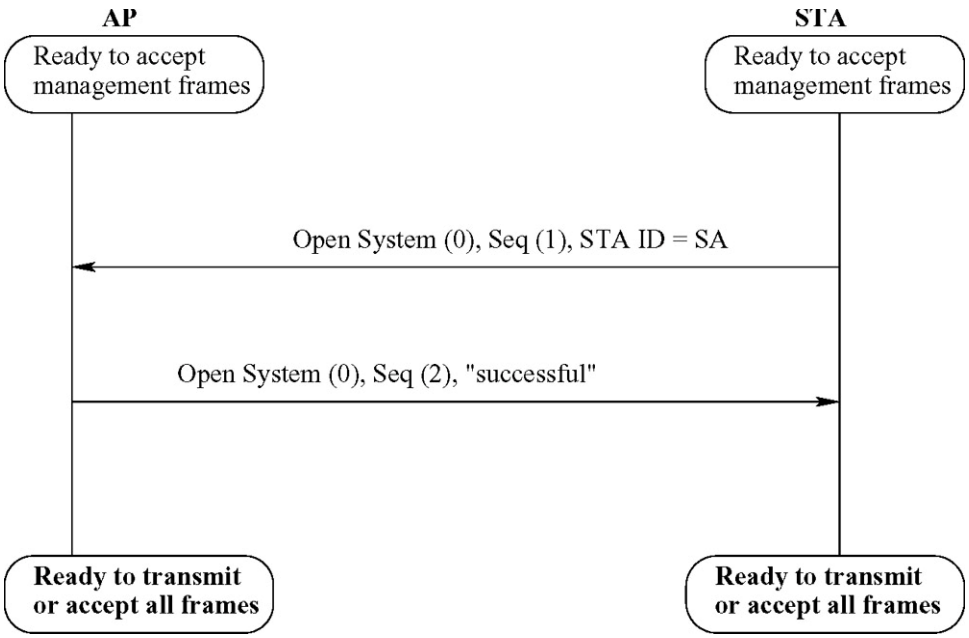
Figur 8 Autentisering i WEP [NIST800-48]

Open System

Open system autentisering er et krav dersom en enhet skal være i samsvar med [802.11-1999]. Metoden er den enkleste av de 2 tilgjenglige autentiseringsalgoritmene.

Standarden refererer til denne som en ”null-autentiserings-algoritme”.

Selv om det ikke foregår noen autentisering av STA, så hevder standarden at det ligger en sikkerhet i at et AP kan velge å avvise en enhet dersom den ikke støtter open system [HAR].



Figur 9 Open System autentisering [HAR]

Dette er en 2 veis utveksling hvor klienten blir autentisert (AP returnerer ”successful”) hvis den sender sin MAC adresse (SA), og AP støtter Open System. Hvis AP ikke støtter metoden returneres ”unsuccessful” og STA slipper ikke inn på nettet.

I praksis foregår det ingen autentisering etter dagens standarder ettersom den ikke benytter seg av noen kryptografiske mekanismer for å autentisere. Dette kan i beste fall med godvilje tolkes som en autentisering, men da bare i form av at man antar at MAC adressen er korrekt. En mer korrekt benevnelse vil være assosiering. Et begrep man finner igjen i [802.11i]

Alle enheter som er knyttet til et open system kan lytte til hverandres datakommunikasjon, og således kan konfidensialitetskravet enkelt brytes.

Shared Key authentication

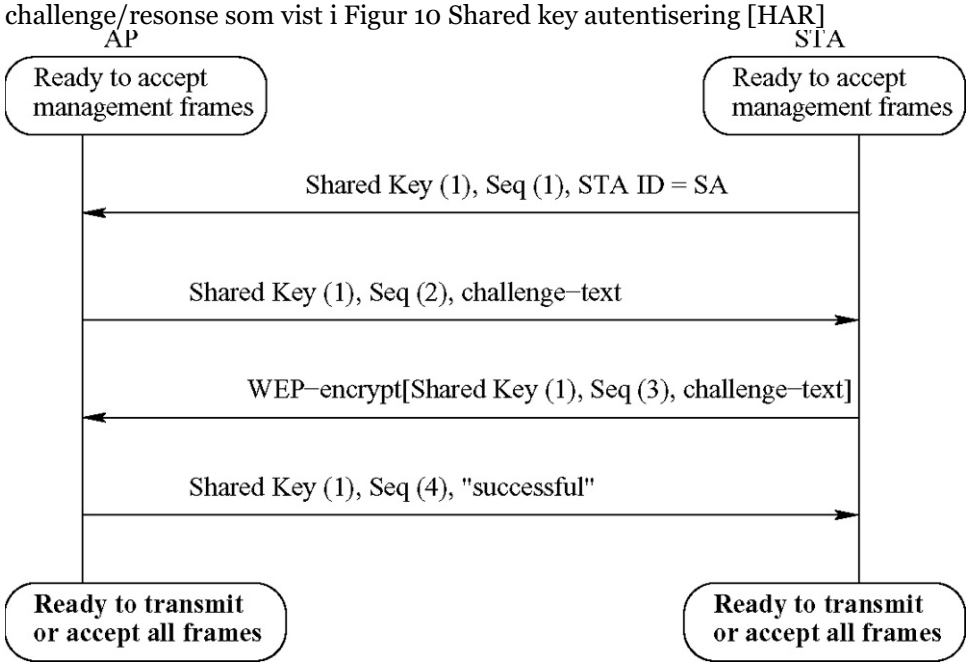
Shared Key autentisering, i motsetning til open system, er ”opsjon[26]” i standarden. Dette betyr at enheter som hevder å være kompatible med [802.11-1999] ikke trenger å tilby shared-key autentisering og fremdeles være i samsvar.

Dersom en enhet skal tilby shared-key autentisering er det spesifisert at denne skal være basert på WEP. Ethvert STA som ber om trådløs tjeneste fra et AP med denne autentiseringsmekanismen, må bevise at det er i besittelse av en hemmelig nøkkel. En nøkkel som er identisk med den noden den skal autentisere seg for. Nøkkelen er

[26] Engelsk: ”Optional”

formodentlig utvekslet via en sikker kanal; en kanal som er uavhengig av og ikke beskrevet i IEEE 802.11.

Shared key autentisering er en 4 veis utveksling, som benytter seg av challenge/resonse som vist i Figur 10 Shared key autentisering [HAR]



Figur 10 Shared key autentisering [HAR]

Identifisering

I den første meldingen ber STA om tilgang til nettverket. Avsenders Authentification Algorithm Identification bit er satt til 1 for å indikere at Shared Key autentisering ønskes benyttet. STA sender også med sin MAC adresse i SA feltet i header. Sekvensnummer 1

Challenge

AP sender en utfordring (challenge) slik at STA kan bevise at den faktisk har identisk WEP-nøkkel som AP. Denne utfordringen er i praksis en tilfeldig tekst. Sekvensnummer økes til 2.

Challenge Response

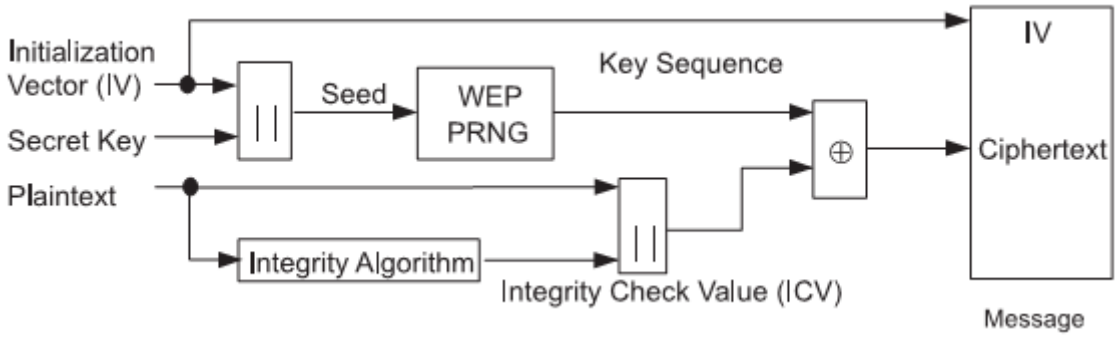
STA svarer på challenge med å konstruere en autentiseringsramme med sekvensnummer 3, og den samme challenge-teksten som den tidligere har mottatt. Den krypterer så dette med WEP nøkkelen og sender den tilbake til AP.

Resultat

Ved mottak av 3. dekrypterer AP meldingen ved hjelp av sin kopi av WEP-nøkkelen. Hvis den dekrypterte meldingen 3 inneholder opprinnelig klartekst som sendt i 2, samt at integritetssjekken av pakken er OK, vil AP godkjenne STA som legitimt og gi tilgang til nettressursene. Sekvensnummerert økes med èn, og sendes til STA med statuskoden ”successful”. Dersom integritetssjekken ikke er OK, eller teksten sendt i 3 avviker fra teksten sendt i 2 vil statuskoden ”unsuccessful” returneres, og STA avvises

4.6.2. Konfidensialitet og integritet i WEP

Krypteringsprosessen



Figur 11 WEP-kryptering [802.11-1999]

Kryptering foregår på lag 2, datalink laget. En pakke på lag 2 kalles en ramme, og i trådløs sammenheng for en MPDU.

MPDU (MAC Protocol Data Unit) og MSDU (MAC Service Data Unit) refererer begge til en enkelt pakke med data med en avsender og destinasjonsadresse og andre variabler. MSDU blir sent fra OS til til link-layer-laget (lag 2) og blir konvertert til MPDU-er som kan sendes over det trådløse nettet. I den mottakene enden vil MPDU-er for deretter å bli konvertert til MSDU-er før det blir sendt til OS-et. Et vesentlig poeng er at èn MSDU kan bli fragmentert til flere MPDU-er på avsendersiden og på mottakersiden blir MPDU-ene igjen satt sammen til èn MSDU. [EDN]

Konfidensialitet

Når WEP er aktivisert i et WLAN, blir hver pakke kryptert individuelt med en RC4 nøkkelstrøm (stream cipher) som blir generert av en 64 bit RC4 nøkkel.

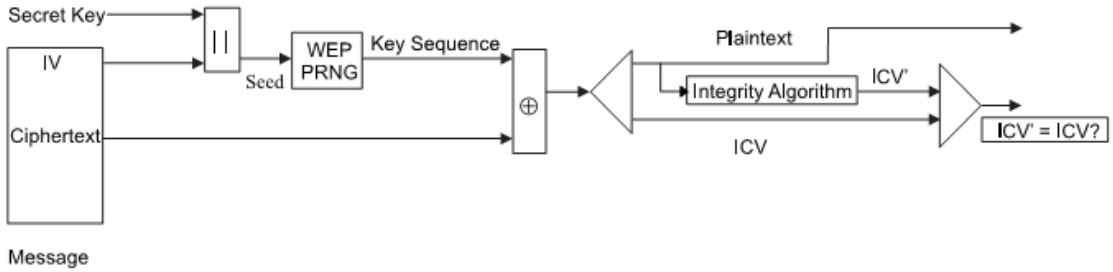
Nøkkelstrømmen genereres av en pseudo random generator (PRNG), av type RC4, med input av en sammensetting av en 24-bits IV og en 40 bits WEP nøkkel, sammensettingen av inputen til WEP PRNG kalles et frø (seed).

Meldingsintegritet

Meldingsintegritet hindrer at pakken blir uautorisert endret under transport. For dette formålet blir klarteksten kjørt gjennom en integritetsalgoritme, CRC32 som produserer en *integrity check value* (ICV)

Kryptering foregår ved å kombinere nøkkelstrømmen med klartekst pluss ICV og addere denne modulo 2 (XOR). Output blir den krypterte teksten pluss IV.

Dekrypteringsprosessen



Figur 12WEP-dekryptering[802.11-1999]

Mottakene STA mottar en kryptert melding. Denne har kjennskap til den hemmelige nøkkelen, og mottar IV ettersom den sendes i klartekst sammen med den krypterte teksten. Ved å sette disse sammen genererer frøet (seed) som kjøres gjennom pseudo random generatoren (RC4) som genererer nøkkelstrømmen. Denne settes sammen med den krypterte teksten og det kjøres en bitvis XOR på denne på samme måte som ved kryptering. Dette gir klarteksten. Som vi ser er dette en symmetrisk krypteringsalgoritme [AGG]

Integritetskontroll gjøres ved klarteksten på mottakers side kjøres gjennom den samme integritetsalgoritmen som på avsendersiden. Dette produserer en ICV' ((ICV merket"). Dersom ICV' er lik ICV så er integritetskontrollen OK. Altså er pakken ikke endret under overføring.

4.6.3. Drøfting av egenskapene

802.11 [802.11-1999] spesifiserer at WEP algoritmen har følgende egenskaper

Den er *rimelig sterk* (reasonably strong).

Sikkerheten ved algoritmen ligger i vanskeligheten med å avsløre den hemmelige nøkkelen ved hjelp av et brute-force angrep. Videre slår standarden fast at godheten av sikkerheten avhenger av nøkkel-lengden og hyppig endring av Initialiserings vektoren (IV)

Den er selvsynkroniserende

WEP er selvsynkroniserende for hver melding. Denne egenskapen er kritisk for krypteringsalgoritmer på datalink laget, hvor pakketapet antas å være høyt

Den er effektiv/egnet (efficient)

Algoritmen kan implementeres i enten programvare eller maskinvare

Den skal kunne eksporteres

I en tid hvor eksport av krypteringsalgoritmer utenfor USA var høyaktuelt, ønsket man å lage en algoritme som skulle kunne være eksporterbar for bruk utenfor USA. Allikevel ga standarden ingen garantier for noe slik.

Den skal være en opsjon

Implementering og bruk av WEP skal være valgfritt

Den hemmelige nøkkelen er konstant, men kan og bør endres, mens IV kan endres for hver pakke. I henhold til standarden kan IV sendes ukryptert siden den ikke gir noen informasjon om den hemmelige nøkkelen. Verdien må dessuten være kjent av mottaker for å kunne dekryptere.

Standarden legger ingen føringer for hvor ofte IV skal endres, men anbefaler at den endres for hver MPDU

PRNG er en kritisk komponent ettersom den omformer en relativt kort hemmelig nøkkel til en vilkårlig lang nøkkelsekvens. I følge standarden forenkler dette nøkkeldistribusjon ettersom det kun er den korte hemmelige nøkkelen som må distribueres mellom nodene (STA).

IV har den egenskapen at den utvider nøkkelens levetid samt at den gir algoritmen selvsynkroniserings egenskap.

4.6.4. Trusselmodell

802.11 hevder å tilby konfidensialitet, gjensidig autentisering, integritets og replay beskyttelse i tillegg til motstandsdyktighet mot DoS-angrep.

[HAR] har utviklet følgende trusselmodell for 802.11.

Trådløs kommunikasjon kan foregå mellom 2 STA eller mellom et AP og en eller flere STA. Man regner at trådløse signaler kan fanges opp i en radius av 100 meter rundt AP, uten spesielt utstyr, og langt utenfor dette med antenner designet for formålet. Således kan kommunikasjonen avlyttes uten å ha fysisk tilgang til nettverket. Derfor er konfidensialitet en et krav.

En ondsinnet tredjeperson kan utgi seg for å være STA eller AP derfor er autentisering og meldingsintegritet et krav.

På tross av kryptert og integritetsbeskyttede pakker kan en ondsinnet spille av gamle pakker (replay) og håpe at disse blir akseptert som nye. Derfor er replay beskyttelse et krav.

Endelig kan ulike metoder for tjenestenektangrep (DoS-DenialOfService) sette nettverket ut av spill. Dette er imidlertid utenfor denne oppgavens rammer.

Mer formelt definerer [802.11-1999] at WEP skal tilby sikkerhet tilsvarende et kablet nettverk; Wired Equivalent Privacy. Eksplisitt hevdes det at standarden ivaretar:

- Konfidensialitet[27]
- Autentisering
- Aksesskontroll

WEPs svar på Trusselmodellen

Designernes hovedmål var å lage sikkerhet for WLAN tilsvarende et kablet ethernet [802.11-1999]. WEP støtter seg på RC4 flytchiffer for konfidensialitet og CRC-32 produserer en checksum (Integrity Check Value - ICV) for integritet. WEP er ikke designet for å beskytte mot tjenestenekt-angrep.

[27] Engelsk: ”Privacy” – i revisjon [802.11i] er dette endret til confidentiality - konfidensialitet

Autentisering av enheten skjer altså når denne kan vise til SSID (Open System) eller WEP nøkkel (Shared Key).

Vi vil i det etterfølgende vise at uansett hvordan man konfigurerer WEP vil ikke disse tre sikkerhetstjenestene kunne ivaretas av WEP. Langt på skyldes dette designproblemer.

4.6.5. Drøfting av mangler i 802.11-1999, pre-RSN

Kravene forsøker å balansere "rimelig sterk" med kravene til enkel implementering og mulighet for eksport. 802.11 sin tilnærming til dette ble en 40 bits WEP-nøkkel. Fra et sikkerhetsperspektiv er det mer naturlig å operere med 2 varianter, nemlig sterk eller ingen. [EDN]

[EDN] forslår at standarden enten skulle spesifisert sterk sikkerhet, eller skulle påpekt behovet for å ha en annen sterk sikkerhetsmekanisme på toppen, for eksempel VPN. Lakonisk slår han imidlertid fast at igjen ble markedskreftene (og muligens også eksportkravet) tillagt større vekt enn sikkerhetsperspektivet.

Kravet til selvsynkronisering er fornuftig, da pakketap, som man må regne med i et trådløst nett, gjør at resten av meldingen kan dekrypteres.

802.11 pre-RSN har imidlertid flere elementære designproblemer som senere har blitt utnyttet til ulike mer eller mindre sofistikerte angrep. Følgende liste er ikke uttømmende, men gir en pekepinn over designproblematikken den opprinnelige standarden introduserer. Denne er vist til i flere kilder; blant annet [VAC], [HAR] og [NIST800-48]

4.6.6. Designproblemer i WEP

WEP lider under flere designproblemer, som har gjort den sårbar for en lang rekke angrep.

Sikkerhetsegenskaper er opsjon

Leverandørene har ikke slått på WEP som standard. Dette bryter imidlertid ikke med standarden hvor WEP er en opsjon, og ikke et krav.

IV er kort

24 bits IV gjør at nøkkelstrømmen gjentar seg. Dette åpner for angrep som ikke trenger å være av spesielt sofistikert karakter Dessuten tilbyr ikke standarden noen retningslinjer på valg av IV. Hvis random IV blir brukt i dette nøkkelrommet er det *sannsynlig* [HAR] at kollisjoner skjer etter noen få tusen pakker på grunn av det såkalte bursdagsparadokset. I tillegg er det et problem at enkelte leverandører leverte nettverkskort hvor IV ble tilbakestilt til null ved reinitialiering, for eksempel ved en omstart av maskinen. Deretter ble IV økt med 1 for hver pakke som ble sendt. Dette gir forutsigbarhet som kan utnyttes.

Nøkler er korte

Standarden spesifiserer at nøkkellengde skal være 40 bit. Slike nøkler er uegnet for ethvert moderne system. Eksempelvis krever datatilsynet at nøkkellengden skal være minst 128 bit, og da for blokkchiffer. Lange nøkler gjør brute force angrep vanskeligere.

Nøkler er delte

WEP bruker vanligvis en felles nøkkel for alle noder i krypteringsdomenet[28]. Dette innebærer at dersom nøkkelen blir kompromittert, eller blir kjent for andre så må alle noder i nettet bytte nøkkel. Dette betinger naturligvis at nøkkelkompromitteringen blir oppdaget, noe som er langt fra sikkert at den blir. Tidsvinduet for eksponering er da potensielt svært lang.

Nøklene kan ikke oppdateres automatisk og ofte

Kryptografiske nøkler bør endres ofte for å hindre brute force angrep. Det mangler føringer for nøkkel administrasjon i standarden. Særlig påfallende er dette når behovet for nøkkelreforhandlinger er åpenbart ettersom nøkkelrommet er så begrenset.

RC4 er dårlig implementert i WEP

Bruken av RC4 i WEP har flere alvorlige mangler. For det første er RC4 et stream chiffer og nøkkelen skal derfor bare brukes en gang for å generere en nøkkelstrøm. For å oppnå selvsynkroniserings egenskapen, som nevnt i standarden anbefales det å bruke en per-MPDU IV for å generere en et per-MPDU frø og en korresponderende nøkkelstrøm. Følgende av dette vil være IV kan endre seg samtidig som nøkkelen er konstant. Således vil det være plausibelt å påstå at nøklene vil kunne ha en del felles egenskaper som gjør at disse kan knyttes til hverandre.

Kombinasjonen av 24 bits nøkkel i IV og en svakhet i RC4 nøkkelstrømmen gjør det altså enkelt å montere et angrep for å avsløre nøkkelen.

Meldingsintegritet er dårlig

WEP bruker CRC32 for integritet. Dette er ikke en kryptografisk sikker integritets algoritme og er svært utsatt for kollisjoner, og er således uegnet som integritetsalgoritme. Kombinasjonen av stream chiffer og CRC32 gjør det relativt enkelt å endre pakker under transport.

Ingen brukerautentisering forekommer

Det er kun enheten og ikke brukeren som autentiseres. Dette innebærer at en stjålet enhet kan aksessere nettverket.

Autentisering er ikke slått på, kun enkel SSID identifikasjon

Det er intet krav til autentisering i standarden. I utgangspunktet skal det holde å kjenne SSID.

Autentisering er enkel shared-key challenge response

Enveis challenge response autentisering er gjenstand for man-in-the-middle angrep.

Klienten autentiserer ikke AP

Ettersom det ikke er noen autentisering av AP er det mulig å bli lurt til å autentisere mot et såkalt rogue AP. Dvs at man kobler seg til et annet AP enn man ønsker. Dette er utgangspunktet for man-in-the-middle angrep.

Kombinert input

[28] Det er i flere implementasjoner støtte for å bruke inntil 4 forskjellige nøkler. Dette utgjør imidlertid ingen større forskjell.

I shared-key autentisering brukes WEP-nøkkelen som input både til autentisering og kryptering. Dette innebærer at brudd på sikkerheten i WEP fører til brudd på både autentisering og kryptering.

4.6.7. Angrep på WEP-protokollen

Som et resultat av dårlig design, som vist over, har WEP blitt kompromittert et utall ganger. Svært mange av angrepene baserer seg på en artikkel publisert i 2001, senere kjent som FMS-artikkelen [FMS]. Arbeidet ble første gang presentert på en sikkerhetskonferanse i juli 2001. På konferansen hevdet man at sikkerheten i WEP-algoritmen var brutt. Deretter viste de matematisk hvordan man kunne utnytte svakhetene i RC4 for å bryte sikkerheten i WEP.

Scott Fluhrer, Itsik Mantin, and Adi Shamir sto bak denne presentasjonen, derav navnet.
Angrep basert på disse funnene ble senere kjent som "FMS angrep" Kort tid etter publisering av artikkelen ble flere verktøy som utnyttet problemene lansert. Blant disse var WEPCrack and AirSnort.

Problemene med RC4 ble sett på som implementasjonsspesifikke for WEP. Uansett hadde kunnskapen som ble lagt til grunn i kryptanalysen publisert allerede 6 år tidligere i 1995 [ROO]

Nylig har tyske forskere vist at en 104-bits[29] WEP nøkkel på unders 60 sekunder [TEW]. Angrepet utnytter kunnskapen som i [KLE] som viste at korrelasjon i forhold til RC4 nøkler var verre enn antatt av [FMS].

"We demonstrate an active attack on the WEP protocol that is able to recover a 104-bit WEP key using less than 40.000 frames with a success probability of 50%. In order to succeed in 95% of all cases, 85.000 packets are needed. The IV of these packets can be randomly chosen. This is an improvement in the number of required frames by more than an order of magnitude over the best known key-recovery attacks for WEP. On a IEEE 802.11g network, the number of frames required can be obtained by re-injection in less than a minute. The required computational effort is approximately 220 RC4 key setups, The actual computation takes about 3 seconds and 3 MB main memory on a Pentium-M 1.7 GHz and can additionally be optimized for devices with slower CPUs. The same attack can be used for 40 bit keys too with an even higher success probability." [TEW]

Som sikkerhetstiltak foreslår de tyske forskerne at WEP ikke bør brukes mer.

Det tilbys mange verktøy, også som fri programvare, som utnytter svakhetene i WEP, disse er meget tilgjengelige på internett. Som en kuriositet finnes det en boks på markedet, med det beskrivende navnet "Slurpr-the mother of all wardrive boxes", som

[29] Vi har tidligere, og med hensikt, kun behandlet 40 bits WEP nøkler da det er dette som er omtalt i standarden [802.11-1999]. På grunn av problemene med WEP ble nøkkelrommet utvidet i senere implementasjoner og markedsført som WEP2. Dette gjør brute-forcing vanskeligere. Men som vist er ikke nøkkellengden det største problemet.

utnytter usikrede nettverk. Informasjonen hos produsenten tilsier at den er kapabel til også å utnytte sikkerhetsproblemene i WEP. Slurpr har 6 mulighet for å aggregere inntil 6 kanaler og i ”teorien” tilby 6x54mbit.

Figur 13 Slurpr the mother of all wardrive boxes

Svakhetene i WEP drøftes ikke videre da det er helt åpenbart, fra et sikkerhetsståsted, at bruken av WEP bør opphøre. For eksempel i den oppdaterte standarden [802.11i] frarådes bruken av shared key autentisering annet enn for bakoverkompatibilitet med pre-RSN utstyr i en migreringsfase til RSN. Vi er av den oppfatning at migreringsfaser har en tendens til å trekke ut i tid. For eliminere dette eksponeringsvinduet anbefaler vi ikke å følge dette rådet, men heller velge å ikke støtte WEP i perioden.

For mindre nettverk, evt hjemmebruk, egner WEP seg kun for å beskytte mot tilfeldige forbindelser, dvs at noen utilsiktet skulle koble seg til. Det anbefales i stedet å benytte WPA-PSK. Denne er langt mer robust, krever ingen ekstra infrastruktur og er like enkel å sette opp som WEP. Majoriteten av utstyr produsert de siste fem årene støtter WPA-PSK, i det minste etter en fritt tilgjengelig programvareoppdatering

For en god oversikt over konkrete angrep som støttes av fri programvare henvises det til annet arbeid. For eksempel gir [HELL] en god oversikt med ”proof-of-concept”. Som en service til leseren gis det en tabellarisk fremstilling av relevante deler av arbeidet til [HELL] i Appendix C

Ellers har [EAR] gode detaljer omkring Stream Cipher attack (FSM), Known plaintext attack, Dictionary Building Attack, Double encryption attack, Message Modification Attack. Depth Attack, ReplayAttacks, Inductive Chosen Plaintext Attack og shared Key Authentication attack henvises til [MIS] Proof of concept er også meget tilgjengelig og detaljert forklart i [CAC]

4.7. Andre lavnivå tekniske sikkerhetstiltak

I en tid hvor WEP har vært eneste alternativ for sikkerhet dersom man ville følge standarden, så har markedet blitt fortalt at gjennom alternative lavnivå sikkerhetstiltak vil summen av beskyttelse, sikkerhet i dybden, være ”sikkert nok” også med WEP som sikkerhetsprotokoll. Eksempler på slike er [SiS]:

Slå av SSID Broadcast

AP forteller om sin tilstedeværelse ved å sende ut sin SSID i et såkalt beacon. Tanken er at dersom man skrur av SSID broadcast blir det vanskeligere for uvedkommende å

vite om nettverkets eksistens. SSID blir likevel sendt når legitime brukere kobler seg til.

Bruke statiske IP adresser

AP kommer med DHCP server og denne er gjerne slått på som standard. Dersom denne slåes av vil inntrenger måtte finne ut hvilket IP-nett han skal tilordne seg en adresse i.

MAC Aksess kontroll lister

Alle enheter som skal opererer i et nettverk må ha en MAC-adresse. Denne identifiserer nettverkskortet og skal være unik. Det vil i de aller fleste løsninger være mulig å konfigurere AP til kun å slippe inn predefinerte adresser på nettverket.

Forfalske SSID

Det finnes programvare for å generere mange falske SSID-er. Tanken er at angriper skal kaste bort tid på å forsøke å knytte seg til et nettverk som faktisk ikke eksisterer. En avart av security by obscurity. Som et alternativ er det ofte anbefalt å ikke bruke virksomhetens navn som SSID.

Antenneplassering

I enkelte sammenhenger, for eksempel [SIS] blir det foreslått at gjennomtenkt antenneplassering kan sørge for en grad av "fysisk sikring" av radiosignalene. Dette kan oppnås ved å plassere AP inn mot midten av bygningen, med lav signalstyrke, slik at de i minst mulig grad stråler utenfor bygningsmassen.

Sticky-page autentisering/Captive Portal tunneling

Autentisering med en nettleser. I praksis er dette et MAC-adressefilter som ofte ses på hoteller og andre steder med behov for såkalte hotspots.

"Sticky-page" autentisering er en avart av MAC-filtrering som i utgangspunktet benyttes for offentlige aksesspunkter (IP-soner eller hotspots). Alle får lov til å koble seg til nettet, men all trafikk blir i utgangspunktet re-dirigert til en spesiell aksesskontrolltjener. Når brukeren har oppgitt betalingsinformasjon/kredittkortnummer (eller autentisert seg på annen måte), legges MAC-adressen inn i en liste over godkjente adresser, og brukeren får surfe fritt i henhold til det han har betalt. [SIS]

4.7.1. Vurdering av sikkerheten i lavnivå tiltak

Det alle disse metodene har til felles er at de ikke gir noen reell beskyttelse mot inntrengere med et minimum av kunnskap. Dette er grundig dokumentert i litteraturen, for eksempel [VLA]. Det beste man kan håpe på er at wardriveren kjører forbi og utnytter andre WLAN i stedet.

Idèen om å forsøke å skjule det trådløse nettverkets tilstedeværelse, gjennom å skru av SSID broadcast, bygger på et kontroversielt prinsipp om sikkerhet gjennom hemmeligholdelse[30]. Det er talløse eksempler i litteraturen, for eksempel [SCH2],

[30] Eng: "Security by obscurity" eller "Security through obscurity"

[VIE], [SCHI] om at dette prinsippet gjentatte ganger spilt falitt og dermed ikke anbefales.

Det er også verdt å merke seg at man den senere tid har oppdaget at det å skru av SSID faktisk kan gjøre sikkerheten dårligere, ettersom AP-ene ikke broadcaster SSID vil arbeidsstasjonene aktivt måtte søke etter disse. Dette kan snappes opp av uønskede personer, som igjen kan bruke informasjonen til å sette opp falske AP, og lure brukerne ti å koble seg til dette i stedet for det legitime nettverket. Dette i kombinasjon med andre metoder, for eksempel en falsk DNS-tjener vil kunne danne grunnlaget for interessante og destruktive angrep. Angrepet kalles i nyere tidsskrift for cloaking-attack, og bygger på arbeidet til [ZOV]. Artikkelforfatterne innarbeidet funnene fra denne artikkelen og implementerte dette i KARMA, som er deres verktøy for testing av sikkerhetsnivå på trådløse klienter. Verktøyet er fritt tilgjengelig fra deres nettsted. Se appendix A.

Det å slå av DHCP-server vil i praksis ikke gi noen økt sikkerhet. Det vil være mulig å finne ut hvilket IP-nettverk som er i bruk ved kun å avlytte noen få pakker med verktøy som for eksempel Wireshark. Flere er nevnt i appendiks A. Det samme vil være tilfelle med MAC-adressefilter i diverse former, som eksempelvis captive portals og sticky page autentisering.

Det er enkelt å avlytte nettverkstrafikk, for å finne og overta en MAC-adresse til en PC som er ”godkjent” på AP [HUR2]

Man kan da velge å sende brukeren av en gyldig MAC-adresse en deauthentication pakke, eller om man skal vente til vedkommende har gått hjem for dagen før man autentiserer seg med sin stjålne adresse [VLA]. I førstnevnte scenario vil brukeren oppleve tjenestenekt, og muligens melde fra til IT-avdelingen, mens i sistnevnte vil sannsynligvis brukeren aldri merke noe.

Captive Portals bruker også i praksis MAC-adresse filterering, og svakhetene ved denne metoden kan uten videre overføres til captive portals. I de fleste implementasjoner av captive portals tillates DNS og ICMP trafikk som standard ut av dette i utgangspunktet sperrede nettet.

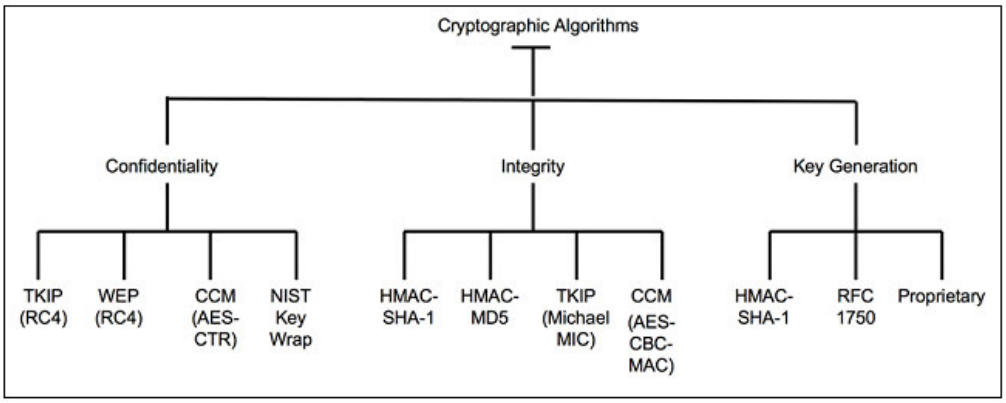
Diverse verktøy kan da brukes for å utnytte dette designet. Dersom man har satt opp en tjener på utsiden, kan trafikk rutes til denne over portene som vanligvis brukes av DNS eller protokoll-nummeret som benyttes ICMP.

Eksempler på slike verktøy er IP over DNS, NSTX OzymanDNS, ICMPTX [CAC]

Angående antenneplassering så faller dette på sin egen urimelighet da man enkelt kan bygge en kraftigere antenne. [OU1] påpeker at antenneplassering og signalstyrke skal optimaliseres for dekning og minimal interference. Og at dette aldri skal brukes som en sikkerhetsmekanisme.

4.8. RSN/802.11i

802.11i/RSN ble ratifisert av IEEE i juni 2004



Figur 14 Kryptografiske Algoritmer[NIST800-97]

Som vist tidligere er WEP under alle omstendigheter usikker. I en tidlig fase mente man at dersom man hadde kompliserte nok nøkler og la på ekstra lag av sikkerhet i dybden, gjennom for eksempel å slå av DHCP, skjule SSID, filtrere på bakgrunn av MAC-adresser eller andre lavnivå tiltak, så ville sikkerheten allikevel være god nok for de fleste.

Ettersom tiden har gått er WEP bevist under alle omstendigheter å være sårbar for en hel rekke angrep, uavhengig av nøkkellengde og "sikkerhet i dybden" med pre-RSN metoder som vist i 4.7.1

Som et svar på dette ble 802.11i standarden laget. Dette som en respons til sikkerhetsproblemene i WEP. Imidlertid lever WEP som sikkerhetsmekanisme videre, men da under betegnelsen pre-RSN.

Ambisjonen med 802.11i var å lage et sikkert rammeverk for tilgang til trådløse nettverk. Dette var helt nødvendig for å imøtegå det enorme antall trusler som begynte å materialisere seg for virksomheter som benyttet seg av pre-RSN løsninger[EAR]

Standarden forsøker å trekke på allerede eksisterende sikkerhetsmekanismer, og bruker et stort antall standarder, protokoller og krypteringsalgoritmer som allerede er definert i og utenfor standarden. Eksempler på dette er RADIUS, 802.1X, EAP, AES, RSN, TKIP. Flere av disse eksisterer som egne RFC-er i IETF.

Sikkerhetstjenestene som tilbys i IEEE 802.11 er:
a)Konfidensialitet;
b)Autentisering
c)Aksesskontroll

Standarden introduserer begrepet Robust Security Network (RSN). Et RSN er nettverk som kun tillater Robust Security Network Associations (RSNA). To noder kan etablere et RSNA dersom de benytter 4-way handshake for autentisering og TKIP/CCMP for konfidensialitet og integritet [EAR]. Dersom man velger å støtte bakoverkompatibilitet med eldre systemer, i praksis WEP, så kalles dette for et pre-RSN nettverk eller Transition Secure Network (TSN) [EAR].

802.11i/WPA(2) finnes i 2 modi, Personal og Enterprise. I hovedsak ligger forskjellene i autentiseringsmekanismene og nøkkelhåndteringsmetodikk. Som det fremgår av navnet er Enterprise metoden beregnet på virksomheter som har infrastruktur til å understøtte denne. Denne vil i det minste kreve en dedikert autentiseringsserver (AS), I praksis en RADIUS-server. Kunnskapen om ulike 802.1X autentiseringsmetoder krever også mye kompetanse i virksomheten for å kunne rulle ut dette på en hensiktsmessig måte.

I stedet for 802.1X bruker personal modus pre-shared keys som PMK i stedet for å utlede disse som et resultat av en EAP-utveksling. Dette er mer håndterbart for virksomheter som ikke ønsker eller har mulighet for å tilrettelegge for en 802.1X infrastruktur.

Enterprise er anbefalt i de fleste situasjoner, ikke bare på grunn av mangelen på muligheter til å kunne differensiere ulike brukere i personal modus, men også på grunn av ulempene og den administrative overheaden med å generere, rulle ut , overvåke og endre pre-shared keys. [NIST800-97]

4.9. Etablering av et RSNA i 802.11i

I dette kapittelet gis det en overordnet beskrivelse av hvordan et RSNA etableres. Deretter vil de delene som er mest relevante for autentisering, konfidensialitet og integritet bli vist.

Som nevnt kan autentisering gjøres ved hjelp av en pre-shared key eller ved hjelp av 802.1X infrastruktur som krever en RADIUS-server med støtte for EAP-protokollen. Dette er analogt med henholdsvis Wi-Fi alliance sin WPA/WPA2-Enterprise-mode og WPA/WPA2-Personal-mode. Personal mode er også kjent som WPA-PSK, hvor PSK står for Pre Shared Key.

802.1X sammen og EAP brukes for autentisering men for å være i samsvar med et RSN må alle noder konfidensialitets- og integritetssikre trafikken med CCMP eller TKIP. Preshared key og 802.1X kan begge brukes og systemet vil fortsatt være i samsvar med kravene for et RSN.

Autentisering kan altså overordnet gjøres på 2 forskjellige måter i et RSNA:
Ved hjelp av en pre-shared key
Ved hjelp av 802.1X; og autentiseringsserver (AS).

I sistnevnte blir Pairwise Master Key (PMK) laget av STA og AS i fellesskap, og denne blir sendt til AP ved hjelp av Authentication and key Management Protocol (AKMP). PMK brukes til å utlede Pairwise Transient Key (PTK), som brukes for å kryptere data mellom AP og STA. Group Master Key (GMK) kan brukes til å avlede en Group Temporal Key (GTK) for å beskytte broadcast og multicast trafikk. [PRA].

Vi vil nå sekvensielt vise prosessen med etablering av et RSNA

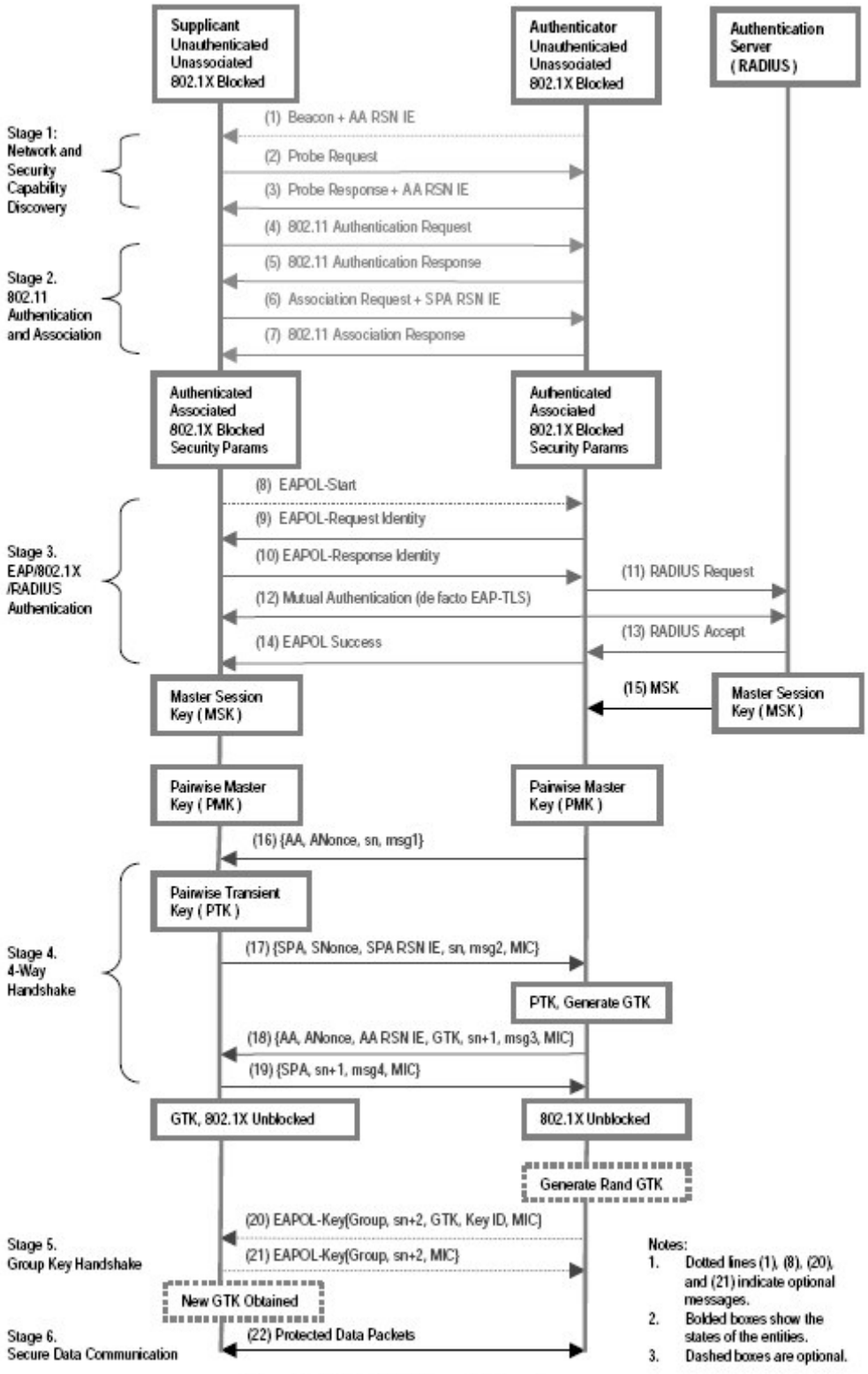


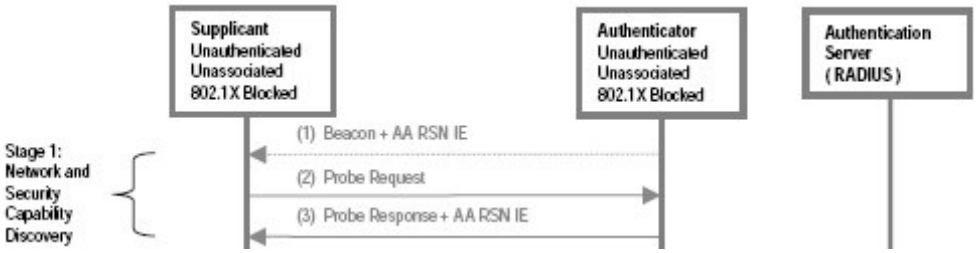
Figure 1. RSNA Establishment Procedures

Figur 15 Etablering av RSNA[HE]

Fase 1 Nettverk og sikkerhetskapabilitets oppdagelse

Denne fasen består av meldingene 1-3.

AP gjør èn av to ting:
a. AP sender med jevne intervaller ut sine sikkerhetskapabiliteter; RSN IE (Robust Security Network Information Element) i et Beacon frame; eller
b. Responderer til en probe request fra STA. Slik:

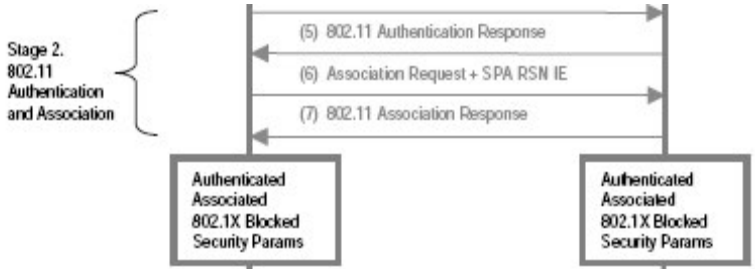


Figur 16 Nettverk og sikkerhetskapabilitets oppdagelse

Fase 2 802.11 Autentisering og Assosiering

Denne fasen består av meldingene 4-7.

STA velger et AP fra sin liste av tilgjengelige AP-er og forsøker å autentisere og assosiere med AP. Dette er så langt relativt analogt med autentisering i et open system som beskrevet i kapittel 4.6.1. Autentisering slik det benyttes i RSNA er beskrevet i neste fase. Det gis ingen tilgang til nettverkets ressurser på dette tidspunkt, utover at STA i neste fase gis anledning til å kontakte autentikator for videre autentisering mot AS.



Figur 17 Autentisering og assosiering

Fase 3 EAP/802.1X/RADIUS autentisering

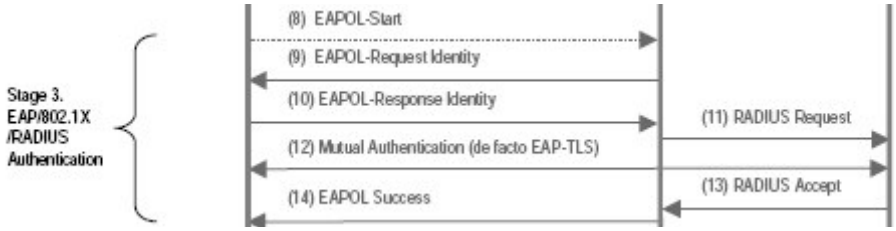
Denne fasen består av meldingene 8-14. Supplikant og AS utfører en gjensidig autentisering ved hjelp av en av de tilgjengelige EAP-metodene. Av EAP-metoder så begrenser denne rapporten seg til følgende.

- EAP-TLS
- EAP-TTLS/MSCHAPv2,

- PEAPv0-MSCHAPv2
- PEAPv1/EAP-GTC
- LEAP

Autentikator (AP) opptrer som et relé inn til AS. Etter denne fasen har supplikant og AS autentisert hverandre og sammen generert en felles hemmelighet, nemlig Master Session Key (MSK). Supplikanten bruker denne til å avlede Pre Master Key (PMK). Nøkkelmateriale på AS blir overført til AP, som vist i melding 15. Dette gir AP mulighet til å avlede den samme PMK.

Dersom STA og AP er konfigurert til å bruke Preshared Key (WPA-PSK, som i WPA Personal Modus) som PMK, vil det ikke være nødvendig med en AS. Man forutsetter da at PSK/MSK blir levert over en sikker kanal. Denne sistnevnte har tilsvarende problematiske egenskap som drøfter under Nøkler er delte i 4.6.6



Figur 18 EAP/802.1X/RADIUS autentisering

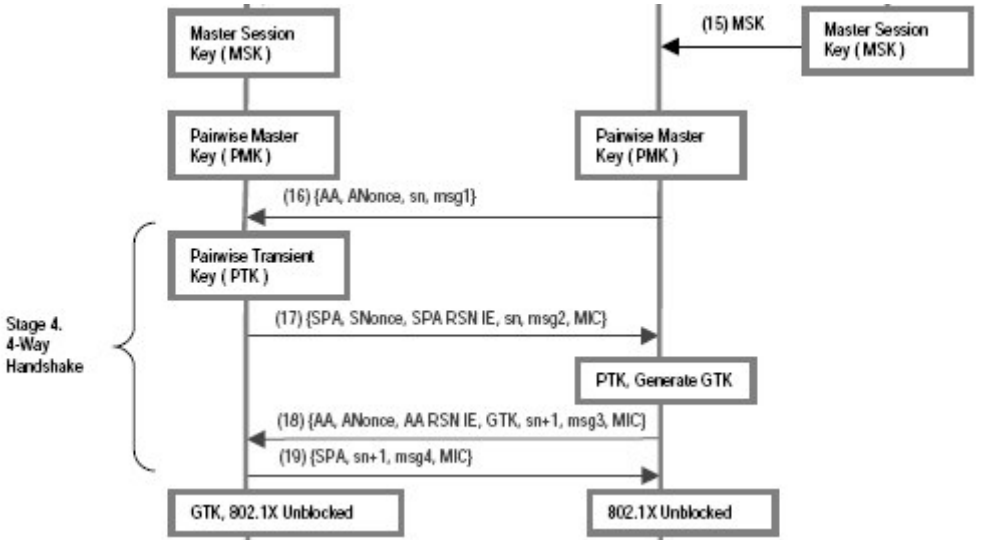
Et vellykket resultat av fase 3, medfører at en PMK Security Association (PMKSA) har blitt etablert. Man tar med seg dette resultatet inn i Fase 4. For detaljer om security association (SA-er) se [802.11i, s62ff.]

Fase 4 4-Way handshake

Denne fasen består av meldingene 16-19.

4-way-handshake må utføres for at det skal kunne være et suksessfull RSNA-etablering. Dette er uavhengig av om PMK er avledet fra fase 3, et resultat av PSK, eller gjenbrukt fra en cachet PMK.

Supplikant og AP bruker metoden for å bekrefte PMK, verifisere valget av krypteringssuite og avlede en fresh Pairwise Transient Key (PTK) for den følgende data sesjonen. For å beskytte broadcast og multicast kan Group Transient Key (GTK) distribueres i melding 18. Etter denne fasen er fresh PTK (evt GTK) delt mellom AP og supplikant og 802.1X porter kan åpnes for datakommunikasjon inn mot nettverkets ressurser.

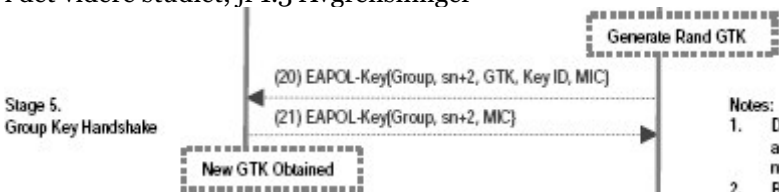


Figur 19 4-way handshake

Et vellykket resultatet av fase 3, medfører at PTK Security Association (PTKSA) og GTK Security Association (GTKSA) har blitt etablert. For detaljer om security association (SA-er) se [802.11i, s62ff.]

Fase 5 Gruppe nøkkel handshake

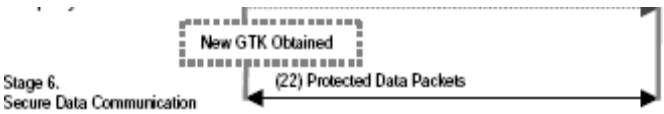
Denne fasen består av meldingene 20-21. I tilfelle multicast applikasjoner, så vil AP generere en fresh GTK og distribuere denne til supplikantene. Disse er ikke nødvendigvis tilstede hvis fresh GTK ble distribuert i fase4; denne fasen kan bli gjentatt mange ganger med den samme PMK. Videre behandling av GTK blir ikke gjort i det videre studiet, jf 1.3 Avgrensninger



Figur 20 Gruppenøkkel handshake

Fase 6. Sikker datakommunikasjon

Denne fasen består av melding 22. Ved å bruke PTK (evt GTK) vil supplikant og AP kunne utveksle data beskyttet av ulike integritets- og konfidensialitetsprotokoller. For et RSNA vil dette være TKIP eller CCMP.



Figur 21 Sikker datakommunikasjon

Vi har nå vist hvordan et RSNA etableres, eller sagt litt uakademisk; hvordan en laptop kan koble seg til et trådløst nettverk etter moderne metoder.

4.10. Konfidensialitet og dataintegritet i 802.11i

Standarden støtter to ulike metoder for konfidensialitet og dataintegritet, nemlig CCMP og TKIP. CCMP er obligatorisk for RSNA-kompatible devicer. TKIP er valgfritt. TKIP er ikke så robust som CCMP i hht standarden, og anbefales kun brukt mot utstyr som ikke støtter CCMP.

I lys av konfidensialitet og integritet skal vi nå se på sikkerhetsprotokollene CCMP og TKIP hver for seg.

4.10.1. CCMP

CCMP, kort for Counter Mode/CBC-MAC-Protocol er basert på CCM modus i AES. CCMP er det som populært betegnes som WPA2 i Wi-Fi terminologi.

CCMP tilbyr konfidensialitet, autentisering, integritet og replay beskyttelse og må være et valg dersom utstyret skal være i samsvar med RSN [802.11i]

CCM ivaretar konfidensialitet gjennom Counter Mode (CTR) og integritet gjennom Cipher Block Chaining Mode with MAC (CBC-MAC) [802.11i].

AES er ikke en sikkerhetsprotokoll, men et blokk-chiffer. I et RSN er CCMP, bygget rundt AES og i kombinasjon utgjør dette en sikkerhetsprotokoll. [EDN]

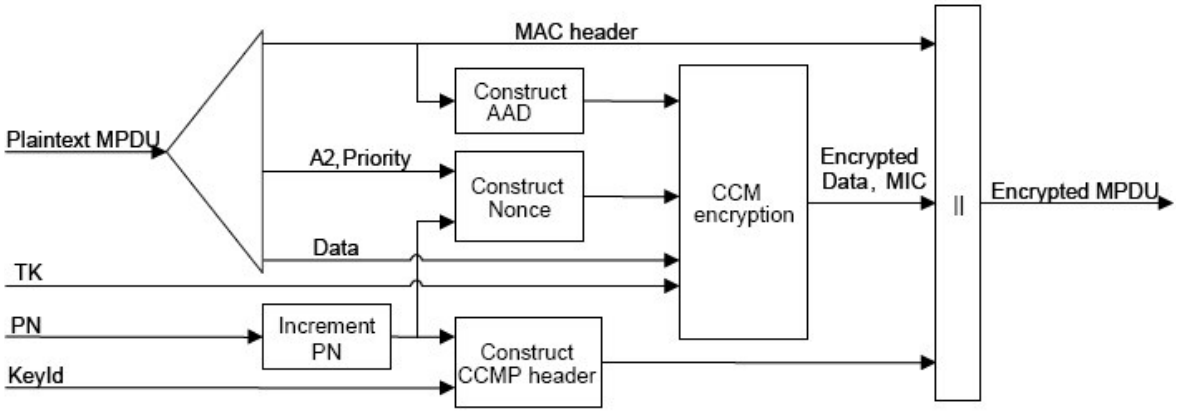
Modes of operation

Metoden for å konvertere mellom en vilkårlig lang melding og en fast blokkstørrelse i et blokk-chiffer kalles operasjonsmodus. Valget av metode er avgjørende for godheten av sikkerheten, og kompleksiteten av implementasjonen. Valg av en dårlig modus, for eksempel Electronic Code Book, kan svekke sikkerheten selv om den underliggende krypteringsalgoritmen er god [SCH2].

På tross av at det er svært mange modi å velge mellom, har Tgi31 spesifisert at kun Counter Mode operasjonsmodus kan brukes, og da i kombinasjon med CBC-MAC.

CCMP enkapsulering

Vi ser her skjematisk hvordan selve krypteringen foregår. For detaljer omkring konstruksjon av AAD, Nonce og MPDU se [802.11i].

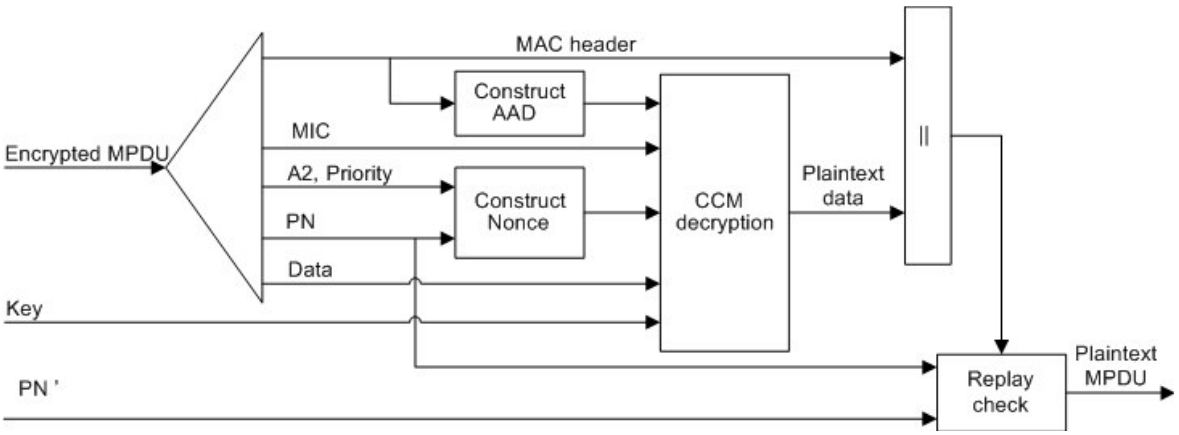


[31] Task Group i – gruppen som jobbet med 802.11i standarden

Figur 22 CCMP enkapsulering [802.11i]

- Sørg for fresh Pakkenummer (PN) pr MPDU ved å inkrementere til et unikt pakkenummer (for sesjonen, egentlig TK)
- Bruk feltene i MPDU header for å konstruere AAD(additional authentication data) for CCM. CCM algoritmen gir integritetsbeskyttelse for feltene i AAD.
- Konstruer CCM Nonce fra PN, A2 og prioritetsfeltet til MPDU. A2 er MPDU adresse 2.
- Legg PN og KeyID i CCMP header
- Konstruer kryptert tekst og MIC fra TK, AAD, nonce og klartekstMPDU
- Konstruer den krypterte MPDU ved å kombinere MPDU header, CCMP header, MIC og krypterte data.

CCMP dekapsulering



Figur 23 CCMP dekapsulering [802.11i]

- MPDU blir behandlet for å utlede AAD og nonce-verdier
- AAD blir utledet fra MPDU header
- Nonce blir utledet fra A2 (MPDU-adresse 2), PN og prioritets-felt (0)
- MIC blir ekstrahert for å brukes til integritetssjekking
- Med input fra TK, AAD, nonce, MIC og den krypterte MPDU utledes klartekst-MPDU. I tillegg sjekkes integritet på AAD og klartekst-MPDU.
- Ved behov rekonstrueres MPDU (sammensetting av fragmenterte MPDU-er og –headere)

Dekrypteringsprosessen motvirker replay av MPDUer ved å validere at PN i MPDU er større enn replay telleren for sesjonen.

MAC-adressen som sendes i klartekst beskyttes mot spoofing av Additional Authenticated Data (AAD). AAD putter header data inn i MIC slik at denne ikke manipuleres.

4.10.2. TKIP

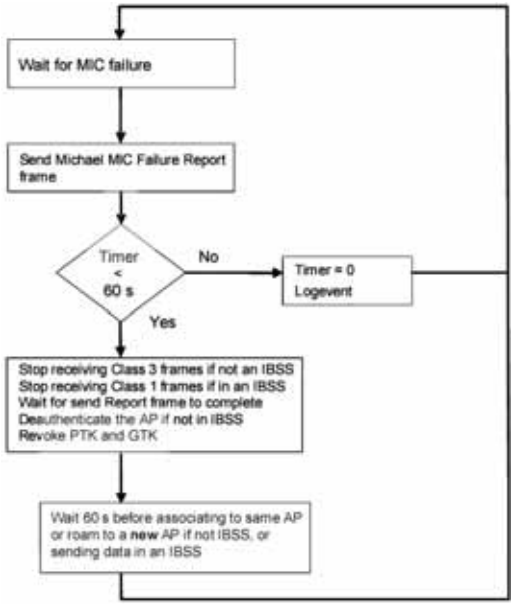
Wi-Fi alliance introduserte WPA i 2003 og var basert på tidlige 802.11i drafts. Hva konfidensialitet og dataintegritet angår har WPA blitt tilpasset og analogt med TKIP. Det har blitt hevdet at TKIP er "WEP i rustning" som håndterer alle kjente problem med WEP [FAL]. Eksempel på dette er at den beskytter mot kjente problemene knytet til RC4 FMS angrep som beskrevet i [FMS].

Målet til TKIP er, ved hjelp av forskjellige teknikker, som vist nedenfor, å rette opp[32] de mange sårbarhetene i WEP, slik at man skulle kunne bruke eksisterende utstyr og kun rulle ut firmware eller software oppgraderinger [HAR]

I henhold til standarden er altså TKIP egnet for å utvide WEP protokollen på pre-RSNA hardware, og forbedrer WEP på følgende:

- I design muliggjør den bruk av 802.1X og EAP, noe som løser problemet med statiske nøkler
- Kalkulerer en MIC over hele ramma ved hjelp av MICHAEL. Denne kan mottaker sjekke etter dekryptering. MIC gir integritet.
- TKIP Sequence Counter (TSC). Hvis pakkene ankommer i feil rekkefølge blir pakka droppet. Dette beskytter mot replay angrep.
- TKIP bruker en S-Box som kombinerer en temporær nøkkel, TA og TSC som input til WEP Seed som vist i kapittelet om WEP. Denne nøkkel mix funksjonen er designet for å overvinne problemene med svake WEP-nøkler
- Utvidet IV fra 24 til 48 bit for å begrense antall kollisjoner
- Design begrensninger i MICHAEL gjør det allikevel mulig for en ondsinnet å bryte dataintegriteten; derfor er det i tillegg implementert mottiltak. Dersom MIC er feil på mottaker siden settes det i gang en timer, og dersom neste MIC feil inntreffer innen 60 sekunder kastes nøklene og ny PTK og GTK genereres. Se Figur 24

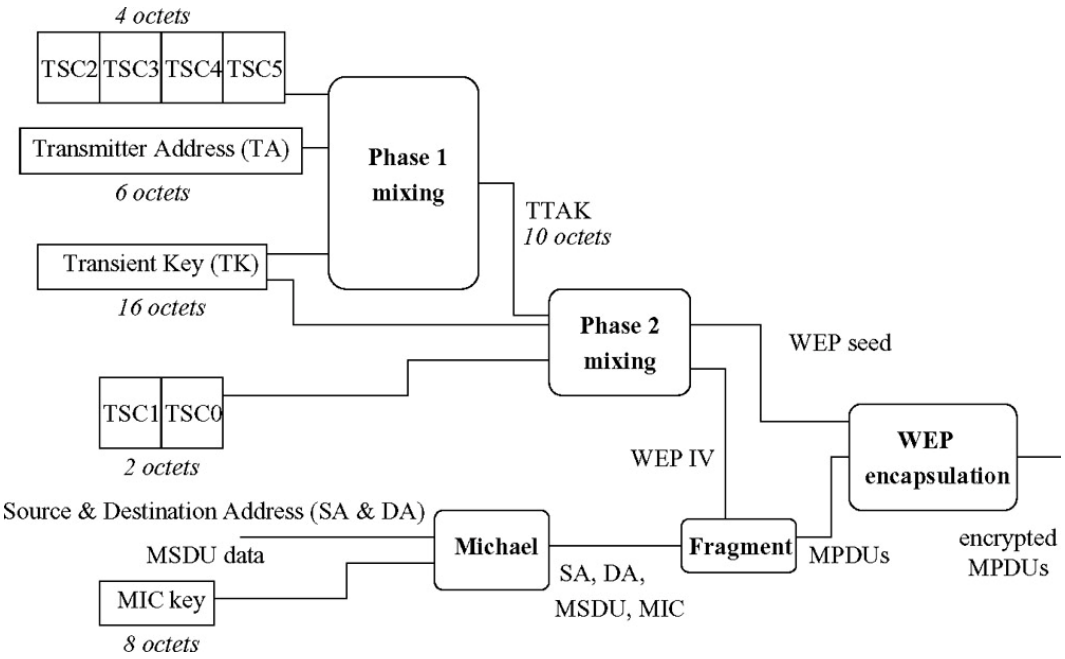
[32] Eng: Patche



Figur 24 TKIP timer[802.11i]

TKIP kryptering

Trinnene i krypteringen er skjematisk slik



Figur 25 TKIP kryptering

Figur 26[HAR]

Trinnene i krypteringen blir da slik

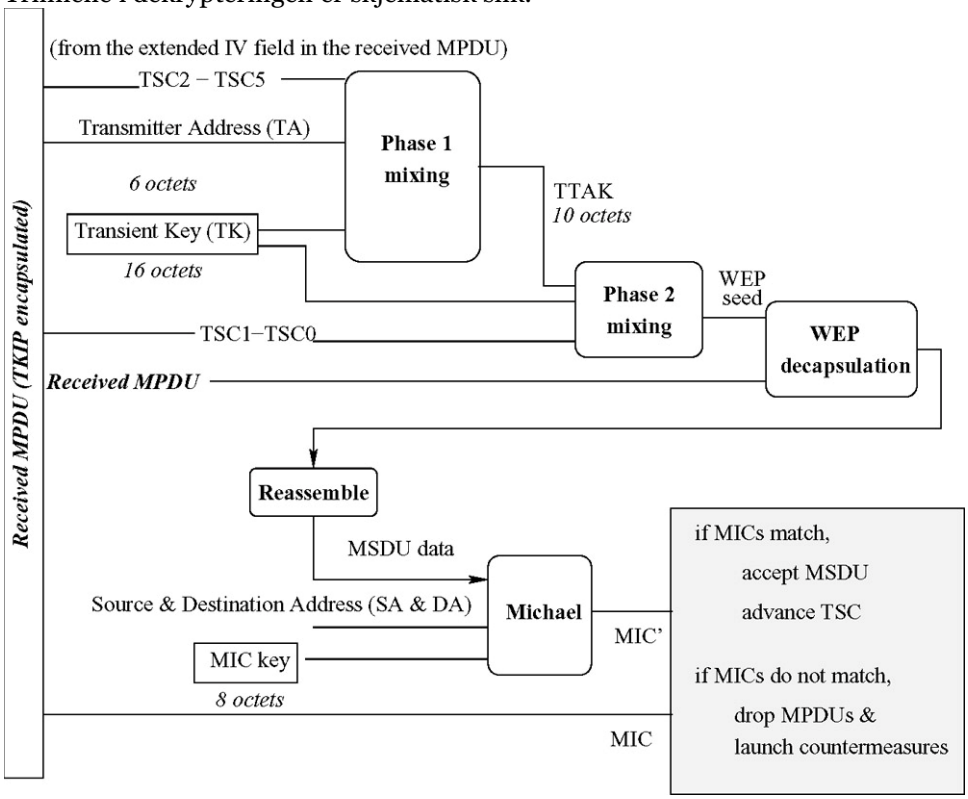
- Avsender genererer MIC, ved hjelp av MICHAEL over avsender-adresse (SA), mottaker-adresse (DA), prioritet, tre reserverte oktetter og selve MSDU-

dataene. MIC oversendes, sammen med MSDU til MAC-laget for ytterligere prosessering

- Ved behov vil MAC-lag-prosessering fragmenterer MSDU pluss MIC til flere MPDU-er før den sender MPDU-ene til TKIP-prosessering
- En monotonisk økende TSC blir brukt for hver MPDU. Denne har til oppgave å beskytte mot replay-angrep i tillegg til at den brukes for avlede en nøkkel for hver MPDU
- TKIP bruker en to-trinns mixing prosess (to S-box-er [802.11i s52] for å avlede en per-MPDU nøkkel for WEP enkapsulering. Resultatet av trinn 1, kalt TTAK, can caches og blir repetert kun for hver 2^16 MPDU.
- Resultatet av mixe-prosessen er et WEP-frø (seed) som blir input til WEP-enkapsulering sammen med MPDU (den fragmenterte MSDU-en som er output fra MICHAEL).
-

TKIP dekryptering

Trinnene i dekrypteringen er skjematisk slik:



Figur 27 TKIP dekryptering

Trinnene i dekrypteringen blir da slik

- Mottaker verifiserer først at MPDU ikke er en replay ved å sjekke om mottatt TSC er kongruent med forventet replay teller samsvarende med SA
- Hvis TSC indikerer at MPDU er fresh, vil mottaker bruke TSC for å beregne per-MPDU nøkkel. Deretter dekrypteres MPDU vedhjelp av WEP

- Hvis WEP ICV sjekk lykkes er klartekst MPDU klar for defragmentering. I motsatt fall blir MPDU droppet.
- Etter defragmentering, beregner mottaker MIC over MSDU, SA, DA, prioritet og de reserverte oktettene. Dersom mottatt og beregnet MIC er kongruente blir MSDU oversendt til høyere lag.
- Mottaker øker replay telleren i samsvar med sist korrekt mottatte TSC.
- Hvis MIC verifikasjon feiler har ve MSDU med korrekt ICV i alle MPDU-er. Det er svært liten sannsynlighet for at alle ICV er korrekte og MIC er feil .

4.11. Drøfting CCMP-TKIP

Forskjellene på CCMP, TKIP og WEP fremstilles her tabellarisk. WEP taes med for oversiktens del.

	WEP	WPA/TKIP	802.11i/WPA2
Krypteringsalgoritme	RC4	RC4	AES
Nøkkelrom	40-bit	128-bit	128-bit
IV	24-bit	48-bit	48-bit
Autentiseringsnøkkel	None	64-bit	128-bit
Integritetskontroll	CRC-32	Michael	CCM
Nøkkeldistribusjon	manuelt	802.1X (EAP) Evt manuelt	802.1X (EAP) Evt manuelt
Nøkkel er unik til	Nettverk	Pakke, sesjon, bruker	Sesjon, bruker
Forhandling av kryptoteknikk	Nei	Nei	Ja
AntiReplay	Nei	Ja	Ja

Tabell 1 Sammenligning av CCMP-TKIP. Basert på [NIST800-97], [LEI], [VAC] m.fl.

En av grunnene til at CCMP blir sett på som sikrere enn TKIP er at sikkerhetsprotokollen ble designet fra grunnen av for tilby sikkerhet for 802.11 WLAN. Designerne i TGi hadde frihet til å designe og bruke de mest anerkjente teknikker for å designe CCMP. Som en kontrast er TKIP et kompromiss for å gjøre det mulig å nyttiggjøre seg av eksisterende utstyr med ”WEP-hardware”. Enkelte deler av TKIP, særlig MICHAEL integritets protokoll har kjente svakheter. [EDN]

Imidlertid har TKIP spesifikke svakheter vært beskrevet [HOL]. Denne type angrep er foreløpig bare mulig dersom spesielle forhold ligger til rette. Artikkelen konkluderer med at sikkerheten i TKIP ikke er brutt, og at ingen praktiske angrep er montert så langt[HAN].

Selv om AES-basert sikkerhet er generelt sterkere enn TKIP-basert sikkerhet, så er TKIP ekstremt sterk og ganske egnet for kommersielt bruk [EDN]

TKIP tilbyr minimalt med sikkerhet på utstyret. Av den grunn burde den betraktes som et minimumskrav. Dessuten kan den degradere ytelsen noe. Fordi den benytter en per-pakke nøkkel [UNI] på maskinvare som er beregnet for tradisjonell WEP.

TKIP tilbyr mottiltak mot kjente angrep på WEP ved å redusere eksponeringstiden til 2 pakker hvert 60. sekund. Som kjent genereres det nye nøkler hvert 60. sekund [HUS]

CCMP derimot krever TK kun for hver sesjon og kun unik nonce for hver ramme som er beskyttet av TK.

AES er for CCMP hva RC4 er for TKIP [EDN]. AES er godkjent som FIPS-standard [FIPS33104-2] og har åpenbart høyeste sikkerhetsnivå av de 2. AES er designet fra grunnen av etter anerkjente prinsipper, mens RC4 er et stream-chiffer som har hatt kjente problemer når anvendt på WLAN. TKIP har sørget for at de kjente problemene har blitt rettet opp.

Begge metodene sender MAC-adressene i klartekst. Ingen av metodene vil således kunne beskytte mot Trafikkanalyse. CCMP kalkulerer imidlertid MIC også over MAC-adressene slik at disse er beskyttet mot spoofing.

AES krypterer og dekrypterer og ganske effektivt og svært sikkert. Det er veldig usannsynlig at fundamentale svakheter vil bli oppdaget/materialisere seg i fremtiden. [EDN]

[HUS] hevder i en artikkel at CCMP, dvs Counter Mode er potensielt sårbar for angrep i måten den konstruerer nonce-et på. Dette er fordi metoden baserer seg på PN, MAC layer A2 feltet og MAC layer prioritets feltet, som input til teller/counter, og kun PN er monotonisk økende. Initiell tellerverdi er imidlertid svært predikerbart, hevder forfatterne, og kan brukes til Hellman's Time Memory Trade Off (TMTO) pre-computation angrep [HEL]. Konsekvensen er at dersom initiell teller ikke er upredikerbar; faller sikkerhetsnivået for AES-128-Counter Mode under den anbefalte grensen for styrken til blokk-chiffer som vist i [GRE]. Forfatterne foreslår en metode for ikke predikerbar PN verdi som de kaller Piggy Back Challenge Based Security Mechanism. Metoden gjør Counter Mode mer robust både mot precomputation og også DoS angrep. Metoden ser imidlertid kun ut til å eksistere på tegnebrettet, og ingen proof-of-concept er vist.

TKIP som bruker WEP som rammeverk bruker et RC4 chiffer med et mye lengre IV-nummer enn WEP. TKIP bruker dynamiske/roterende 128-bits nøkler, og har dessuten MIC for å sikre meldingsintegritet.
Selv om dette er et stort skritt i riktig retning; den hevdes å eliminere alle problemer med WEP, så mangler den fremdeles brukerautentisering og tilbyr dermed ikke den sikkerheten som er forventet av mange brukere.[RIT-kap10.6] - NB gjelder for WPA-PSK

Hole et al [HOL] viser i en artikkel at det finnes et potensielt angrep på den temporære nøkkelen i TKIP sin mixe funksjon. Motstandsstrategier og konsekvenser for angrepet skisseres i [HAN] [MOE]

[33] FIPS-Federal Information Processing Standard

> "If anybody breaks TKIP, they not only break the confidentiality but they also break the access control and authentication so one break breaks everything. That is not good design. Each security mechanism should stand on its own" [MIS2]

Av sitatet over kan vi slutte at dette er en svakhet som er arvet fra WEP. Nyere litteratur er relativt samstemt om at TKIP er en midlertidig løsning hvor man "kurerer symptomet og ikke årsaken". Som en konsekvens av dette bør den kun brukes i en overgangsperiode.

CCMP på sin side er designet fra bunn med bruk av anerkjente algoritmer for konfidensialitet og integritet. Prinsippet kalles gjerne "secure by design".

Det vil altså ikke være kontroversielt å hevde at dersom man rangerer godheten av sikkerheten i de tre metodene for konfidensialitet og integritet vil listen fremkomme slik. Beste først:

1. CCMP
2. TKIP
3. WEP

4.12. Autentisering

Sentralt i alle nettverkssystemer er autentisering. Vi vil nå se på hvordan autentisering er håndtert i 802.11i

Definisjon Autentisering: Bevis på hvem man er basert på minst èn av faktorene under

I henhold til [BIS] og de flere andre autoriteter på området, vil autentiseringsteknikkene være basert på og ha en eller flere av følgende egenskaper, eksempler i parentes:

- Noe du vet (brukernavn og passord)
- Noe du har (aksess token, smartkort)
- Noe du er (biometriske metoder)
- Hvor du er (på en spesiell maskin)

Det bør nevnes at ikke alle autoriteter er enige om den siste egenskapen, noe som heller ikke er beskrevet i standardene omkring 802.11i sikkerhet. Denne egenskapen kan realiseres i et WLAN som et MAC-adressefilter, men har liten til ingen relevans i et 802.11i nettverk. Det blir derfor ikke videre behandlet her.

Der det er behov for trygg og sikker autentisering er det behov for å kombinere to av disse egenskapene [DAL]

Tilsynelatende bør det ikke være store problemer for brukerne å holde autentiseringsakkreditiver skjult. Imidlertid er det slik at den enkelte etter hvert har ervervet en enorm mengde brukernavn og passord. Dette er av en slik størrelsesorden at det er umulig for den enkelte å memorere samtlige. Brukerne tyr derfor til enkle løsninger. Problemet er at disse løsningene svært sjelden er forenlig med god

sikkerhet. I tillegg til dette er det, i et flerbrukersystem, slik at mange brukere har tillit til at systemet og sentrale IT-personer håndterer sikkerheten for dem.

Den mest utbredte formen for autentisering i et informasjonssystem er utvilsomt brukernavn og passord [NWF] [CSI06], [CSI07]. Når man da vet at en bruker trenger et passord for hver eneste tjenestetilbyder, er det opplagt at passordhåndtering er en administrativ utfordring for den enkelte bruker. Konsekvensen er at brukeren velger en av følgende strategier:

Skrive ned passordene på papir eller fil
Bruke ett passord på alt, dersom mulig
Lar en applikasjon håndtere/lagre passordene

Disse strategiene har til felles at brukeren eller systemet ikke må avsløre passordene til utenforstående.

Dersom man ser på utbredelsen av passord som autentiseringsmekanisme, er det lett å se at gevinstpotensialet ved å bedre sikkerheten og bevisstheten rundt denne er enorm.

NTA Monitor deler i en undersøkelse [NTA] opp brukerne i tre grupper. I gruppen for ”tunge brukere”, dvs en gruppe med gjennomsnittlig 21 passord, har 49 % passordet skrevet ned på papir eller i ei fil på PC’en. De ”lette brukerne”, som i gjennomsnitt har færre enn 5 passord å håndtere er tallet 31 %. Det er tydelig at de som har mange passord å administrere har en tilbøyelighet til å skrive disse ned.

Hver gang et passord brukes, øker risikoen for kompromittering, og således reduseres dets sikkerhet hyppig sier [PIE]. Av dette kan det sluttes at strategien med å bruke det samme passordet overalt, vil sikkerheten relativt sett, reduseres omvendt proporsjonalt med antall innlogginger. Tidsvinduet fra tilfredsstillende sikkert til lav sikkerhet vil derfor være kort. Hvor kort avgjøres blant annet av hyppigheten av innlogginger, eller innloggingsfrekvens.

Dersom brukeren har valgt, for ham den behagelige strategien, med ett passord overalt, vil ringvirkningene blir store dersom trusselen materialiserer seg, ettersom dette ene passordet vil gi tilgang til alle tjenester brukeren benytter seg av.

Hver for seg har metodene ovenfor svakheter. Førstnevnte kan kompromitteres på forskjellige måter, f.eks gjennom tekniske tiltak som ordliste og brute-force angrep på passordet, i tillegg til eleganse i form av sosial ingeniørkunst eller mer brutal utpressing. Et statisk passord har dessuten den svakheten at det finnes metoder for å avlese passordet når det skrives inn, såkalte keylogger som finnes både som programvare og små maskinvareenhter som kobles på mellom tastatur og maskin.

Å basere seg kun på egenskapen, noe du har, er lite hensiktsmessig da besittelse av enheten, for eksempel et hardware token eller et smartkort vil gi tilgang. Egenskapen må kombineres med noe annet, for eksempel en PIN-kode.

Noe du er, i praksis biometri, har svært mange aspekter ved seg som gjør teknologien problematisk og er utenfor det som uten videre støttes i Wi-Fi autentisering. Det finnes imidlertid proprietære løsninger for dette, som vi så vidt kommer inn på.

Brukte sikkerhetsteknologier i [CSI05], [CSI06], [CSI07]

	Token	PKI	Biometri	Statiske passord
2005	42	35	15	
2006	35	36	20	45
2007	37	32	18	51

Tabell 2 Prosentvis andel av respondenter som bruker metoden for å gi tilgang.

Som vi ser i Tabell 2 er statiske passord mest utbredt for å gi tilgang til virksomhetsdata.

4.12.1. To-faktor autentisering

Det er altså klare svakheter, å bare å basere seg på kun en av disse metodene. Eller som uttrykt i [DAL]

Der det er behov for trygg og sikker autentisering er det altså behov for å kombinere to av disse egenskapene.

Av autoriteter refereres denne kombinasjonen til som såkalt to-faktor autentisering. Og vil være det opplagte valget for de som i sin sikkerhetspolicy behandler et WLAN som et eksternt nett. Påstanden har bred støtte av autoriteter, for eksempel [SUM], [EDN] [HOF] [PFL], [GOL].

De mest utbredte metodene for to faktor autentisering er bruk av smartkort med en PIN-kode eller en PIN kode i kombinasjon med et engangspassord, oftest kalt OTP[34] eller et Token.

Med passord som eneste autentiseringsmetode er konsekvensen av en stjålet eller tapt datamaskin eller PDA fullt sikkerhetsbrudd dersom passordet avsløres.

En undersøkelse fra januar 2005 viser at problemet med bortkomne laptoper er enormt. i løpet av andre halvår 2004 ble det gjenglemt 4973 bærbare datamaskiner i taxiene i London (foruten 63 135 mobiltelefoner og 5838 PDA-er). En økning på 71 % på 3 år [REG][35]

En annen positiv effekt av to-faktor autentisering er at brukerne *tvinges* til aktivt å ta del i autentiseringen. Dette vil kunne virke preventivt på utilsiktet nettvandring.

A clever solution that avoids human weakness is the use of the one-time password [EDN].

[34] OTP-One Time Password

[35] Det bemerkes at undersøkelsen er initiert av Pointsec som er en leverandør av krypteringssystemer for datamaskiner. Pointsec er senere kjøpt av Check Point

"Another great way of addressing this problem is to use two-factor authentication, such as RSA tokens. A mobile PDA user who enters their username and PIN plus a one-time passcode instead of a static password wouldn't be exposing a password that could be used again by the hacker. For that reason, every corporate […] should utilize two-factor authentication" [HOF]

Selv om påstandene fra [HOF] er hentet fra et miljø som fokuserer på å aksessere virksomhetsdata over det mobile telenettet, vil likheten, og ikke minst konvergens, gjøre at påstanden også vil ha gyldighet for 802.11 trådløst miljø. Det er også verdt å merke seg at denne fokusen først har blitt gjenstand i et trådløst miljø i denne utgivelsen, medio 2007

Når vi ser dette opp mot alternative metoder under EAP har vi følgende relevante kombinasjoner i Tabell 3 :

Kombinasjoner	EAP-metode	Standard/proprietær
Passord+OTP	EAP-GTC	Standardisert under Wi-Fi
Passord+Smartkort	EAP-TLS	Standardisert under Wi-Fi
Passord+Biometri	Proprietær	Bio-NetGuard
Biometri+Token	n/a	Ikke kjent

Tabell 3 kombinasjoner av to-faktor autentisering og EAP-metoder

4.12.2. OTP som en del av en to-faktor løsning

I en OTP-løsning autentiserer man seg med en kombinasjon av en PIN-kode (noe du vet) og en dynamisk generert streng fra tokenet (noe du har).

Passordene i en OTP-løsning blir generert på bakgrunn av pseudo-random-number-generatorer og er dermed mer robuste mot angrep, de skifter ofte typisk hvert minutt noe som reduserer tidsvinduet for "over-skulderen-angrep" dramatisk. Metoden kalles som oftest "liveness" i litteraturen, i dette tilfellet at en del av input til passordet er noe som endres ved faste intervaller [EDN].

Et eksempel er RSA SecurID som kombinerer et frø (seed) med tidspunktet for å generere en unikt pseudo random kode (nonce) [RSA]. Andre fabrikanter med stor installert base for engangspassord er produktlinjene til Vasco og Verisign, henholdsvis Digipass og Verisign OTP. Metodene er i samsvar med standarden [PKCS#15].

OTP kan også befinne seg som programvare på en mobiltelefon eller en PDA, alternativt kan denne tilsendes pr SMS. Sistnevnte har klare utfordringer, både i forhold til sikkerhet og funksjonalitet, men omtales ikke videre her.

Verisign OTP

Vasco Digipass G03

Vasco Digipass Pro 250

RSA SecurID 700

RSA SecurID 900

"PDA-Style"

Selv om bruker har lagret sin del av passordet på laptopen, vil et tap av denne ikke kunne gi tilgang, ettersom resten av passordet sannsynligvis befinner seg på brukerens nøkkelring. EAP-GTC metoden kan brukes sammen med OTP.

4.12.3. Smartkort som en del av en to-faktor løsning

Smartkort er typisk i kredittkortstørrelse og inneholder en liten mengde minne evt i kombinasjon med en prosessor. Dersom en slik løsning skal tas i bruk i vår kontekst, er det for å oppbevare den privat nøkkelen i en PKI-løsning på et eksternt medium. Denne låses opp med et passord eller en PIN-kode, alternativt i kombinasjon med biometri. Dersom biometri tas i bruk i tillegg til passord eller PIN, har vi i praksis en tre-faktorløsning [VAC]. For konsistensens del omtalervi allikevel smartkortløsninger som to-faktor i det følgende. Løsningen anbefales brukt i virksomheter hvor høy sikkerhet er en nødvendighet [VAC].

Figur 28 Smartkort

EAP-TLS metoden kan brukes sammen med smartkort.

4.13. Autentisering i 802.11i RSN.

Autentisering i et RSN kan på et helt overordnet nivå baseres på en av to ulike løsninger. Nemlig en såkalt "personlig modus" eller en "virksomhetsmodus[36]".
I førstnevnte benytter hele organisasjonen en forhåndsdelt nøkkel, en såkalt pre-shared-keys (PSK). Sistnevnte baserer seg på bruk av rammeverket 802.1X [IEEE802.1X] for transport av autentiseringdata[37] ved hjelp av Extensive Authentication Protocol (EAP) over WLAN og LAN. Fra et infrastrukturelt ståsted vil personlig modus skille seg fra virksomhetsmodus ved at sistnevnte, i tillegg til det trådløse aksesspunktet, krever en autentiseringsserver med støtte for aktuell EAP-metode, se appendix B. Dette er i de aller fleste installasjoner en RADIUS-server. Rammeverket for 802.1X standarden er konseptuelt svært enkelt, nemlig å hindre en maskin å koble seg til nettverksressurser før brukeren på denne er autentisert.

Ettersom 802.1X og EAP har sentrale rolle innenfor RSNA vil vi gå igjennom dette relativt detaljert.

Nødvendige begreper i denne sammenheng er, avledet av definisjoner i [KNA],[802.1X]:

Supplikant

Enheten som legger fram informasjon som bekrefter enhetens identititet. I praksis klientprogramvare på STA. Supplikanten kan følge operativsystemet. Supplikanten for Windows XP og Windows Vista har som standard støtte for EAP-TLS og EAP-PEAPv0-MS-CHAPv2.

Autentikator[38]

Enheten som kommuniserer med supplikanten og krever autentiseringsinformasjon som den videreformidler til AS. I kontektsten WLAN vil det være aksesspunktet som har rollen som autentikator. I større, profesjonelle virksomhetsløsninger vil autentikator kunne være en kontroller for alle aksesspunktene. I praksis vil denne kontrolleren konfigurere alle aksesspunktene for å videresende alle forespørsler til seg. All drøfting her bruker imidlertid AP eller autentikator. I et virksomhetsnettverk vil en kontrollerbasert løsning muliggjøre enhetlig og sentralisert konfigurasjon av AP-er, noe som i seg selv kan gi en sikkerhetsmessig gevinst i tillegg til å forenkle konfigurasjon og administrasjon av AP-er betraktelig. I vår kontekst derimot, sikkerhetsprotokoller, vil ikke dette utgjøre noen prinsippiell forskjell.

Autentiseringsserver(AS)

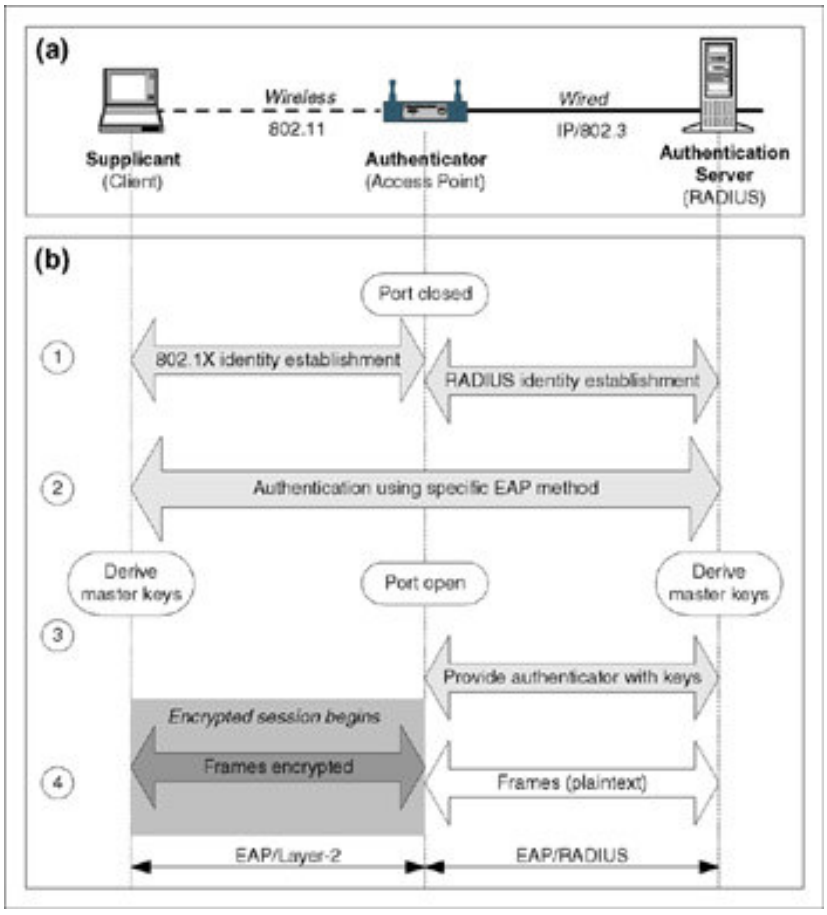
Enheten som verifiserer identiteter og autentiseringsdata og som godkjenner eller avslår supplikantens forespørsel om å slippe inn på nettet. I konteksten WLAN i dag vil AS være ekvivalent med en RADIUS-server. En forbedring av RADIUS-server er

[36] Wi-Fi Alliance omtaler dette som henholdsvis Personal Mode og Enterprise Mode

[37] Med autentiseringsdata forstås her dataene som bekrefter en identitet, f eks en antatt unik kombinasjon av brukernavn og passord eller et X.509 sertifikat.

[38] [KNA] bruker begrepet *autentiserer* om autentikator. Imidlertid er det ikke denne enheten som står for autentiseringen, noe begrepet autentiserer skulle tilsi. Vi velger derfor å bruke autentikator, oversatt fra engelsk; authenticator.

tilgjengelig og har fått det beskrivende navnet DIAMETER. Sistnevnte er imdlertid lite utbredt. I denne sammenheng er AS ekvivalent med RADIUS.



Figur 29 Entiteter og nøkkeletablering[HAR]

4.13.1. Kommunikasjonsflyt i 802.1X

Mellom supplikant og AP brukes initielt EAP/Layer2, dvs EAP over LAN (EAPOL), enkelte steder kalt EAP over Wireless. Mellom AP og RADIUS brukes EAP over RADIUS.

I Figur 29 Entiteter og nøkkeletablering[HAR] vises grunnleggende kommunikasjonsflyt.

- Når en ny supplikant forsøker å koble til aksesspunktet, så åpner AP opp èn port
- AP tillater kommunikasjon over denne porten inn mot AS (i praksis RADIUS)
- All annen trafikk enn RADIUS mot AS er blokkert inntil brukeren er autentisert

- 802.1X supplikanten kobler seg til over Extensible Authenticaton Protocol (EAP), for å autentisere med RADIUS
- Autentiseringen vil[39] være 2-veis, klienten og nettverk
- Avslutningsvis utveksles nøkkelmateriale for kryptering av resten av trådløskommunikasjonen
- Først etter autentiseringen av brukeren vil nettverkets ressurser være tilgjengelig

[BRI]

Beskrivelsen kan med fordel ses i sammenheng med beskrivelen i 4.9 Etablering av et RSNA i 802.11i.

4.13.2. Fordeler med 802.1X

Krever ingen spesifikk protokoll for autentisering, ettersom den er en enkapsulerings-protokoll som tillater ulike autentiseringsprotokoller. EAP kan sies å være en kanal for andre autentiseringsprotokoller som RADIUS, Kerberos og SecurID. [VAC]. I dagens RSN er det RADIUS som benyttes. RADIUS har typisk en kobling mot en brukerdatabase enten intern, eller ekstern i form av Microsoft Active Directory (AD) eller Novell eDirectory. På denne måten slipper man å vedlikeholde to eller flere brukerdatabaser. Aktuelle autentiseringsdata i vår kontekst vil være de fem EAP-metodene som er beskrevet i 4.14.

[VAC] trekker frem følgende som fordeler med 802.1X

- Basert på IEEE Standard– [802.1X]
- Fleksibel
- Skalerbar til store virksomhetsnettverk
- Sentral administrasjon
- Krypteringsnøkler er dynamisk generert og propagert
- Roaming/nettvandring kan gjøres tilnærmet sømløst
- Innebygget støtte i Microsoft Windows XP

4.14. EAP-Metoder

Utvalget EAP-metoder er stort, samtidig som det er svært viktig å velge riktig EAP-metode.

Organizations have considerable discretion in choosing which EAP methods to employ; a poor EAP method choice or implementation could seriously weaken an IEEE 802.11 RSN's protections.[NIST800-97]

[RFC2284], som var den opprinnelige "EAP-RFC-en" drøfter mange EAP-metoder, men da over Point-to-Point Protocol (PPP) [RFC1661]. Eksempler på dette er MD5-Challenge, One-Time Password (OTP) og Generic Token Card (GTC; type 6). Som det fremgår av spesifikasjonen var PPP designet for ende-til-ende kommunikasjon. I konteksten trådløse nett er ikke metodene i [RFC2284] lengre egnet i sin opprinnelige

[39] I metoder godkjent av Wi-Fi Alliance som vi avgrenser til i denne rapporten

form, da deres natur gjør dem uegnet for å håndtere de trusler som blir introdusert i et trådløst nettverk. Vi vil i det etterfølende drøfte følgende metoder, som er relevante i forhold til WLAN-trusselbildet:

- EAP-TLS
- EAP-TTLS/MSCHAPv2
- PEAPv0/MSCHAPv2
- PEAPv1/EAP-GTC
- LEAP

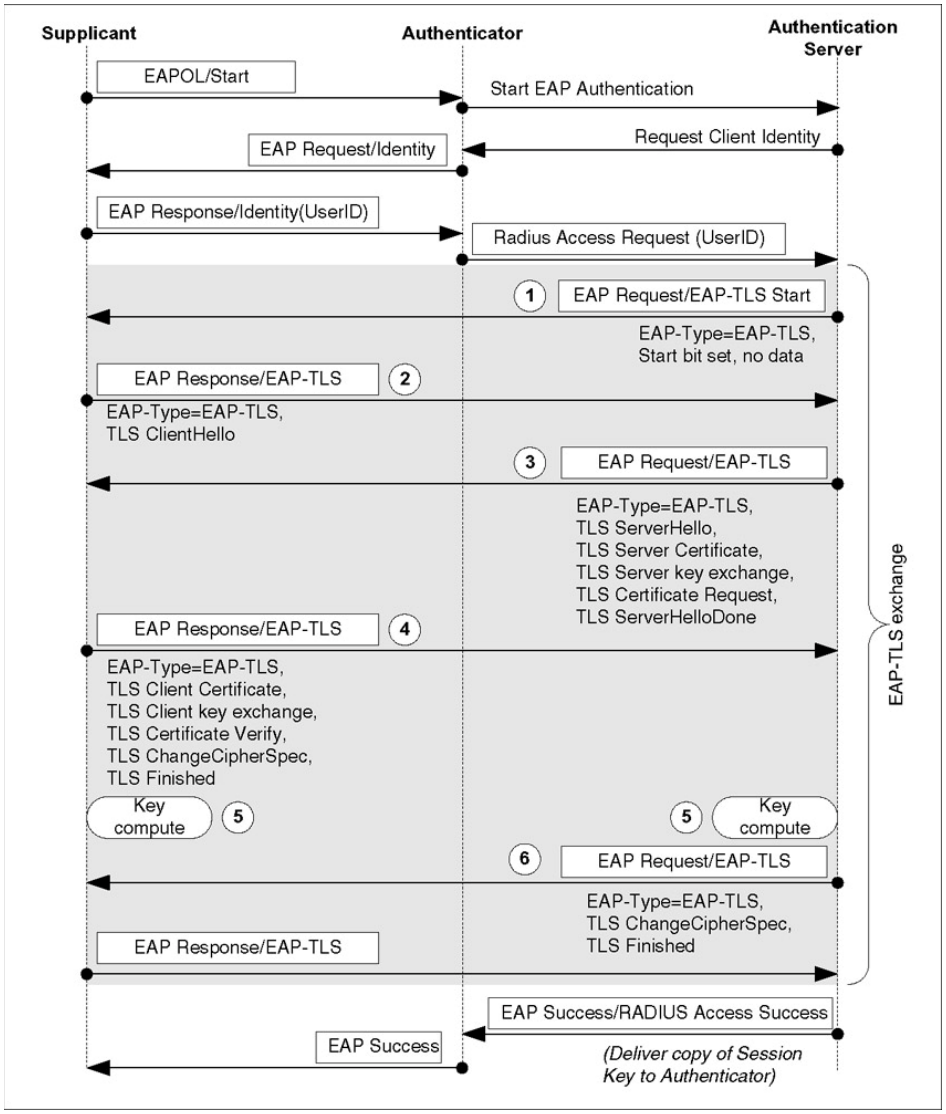
For at utstyr skal kunne sertifiseres av Wi-Fi Alliance i dag må de støtte de 4 førstnevnte. Det er også krav om støtte for EAP-SIM for Wi-Fi sertifisering. Denne er lite utbredt og er beregnet for kommunikasjon basert på SIM-kort i GSM-telefoner. Dette er utenfor fokus for denne rapporten, og behandles derfor ikke her.

LEAP er proprietær for Cisco Systems. Denne blir også drøftet ettersom den er, eller i det minste har vært, svært utbredt. Årsaken er at det var en av de første kommersielle løsningene som tok i bruk 802.1X rammeverket, noe som overflødiggjorde statiske WEP-nøkler.

4.14.1. EAP-TLS

Fram til mai 2005 var dette den eneste EAP-metode som måtte være implementert for å bli sertifisert av Wi-Fi allicance. Løsningen krever full PKI-infrastruktur og sertfikater både på AS og på supplikant-siden. Dette er den eneste av de omtalte EAP-metodene som har status som RFC-standard [RFC3748]

Grunnleggende EAP-TLS utveksling er vist i Figur 30.



Figur 30 EAP-TLS utveksling[HAR]

Før selve EAP-TLS utvekslingen begynner mottar AS klienten sin identititet i svaret på sin request, slik:

Request Dette er starten på EAP utvekslingen. AS ber om identiteten til klienten
Response Her sender klienten en melding med sin identitet til AS

1. EAP Request/EAP-TLS Start
AS sender en tom EAP-TLS request med start bit satt. EAP-Type er satt til EAP-TLS
2. EAP Response/EAP-TLS
Supplikanten sender Client Hello med den samme informasjon som for en ordinær TLS-pakke. Dvs supplikantens TLS versjonsnummer, sesjons ID, et nonce, og hvilke cipher suites den støtter.
3. EAP Request/EAP-TLS
AS sender to eller tre TLS meldinger i en enkel request. Server hello, AS Server sertifikat, evt request for klient sertifikat og Server HelloDone.
4. EAP Response/EAP-TLS

Supplikant svarer med flere TLS meldinger i en respons: Klient Sertifikat (signert med klientens private nøkkel), nøkkelutvekslings parametre, utregning og oversending av pre-master secret (kryptert med AS sin offentlige nøkkel).

5. Key Compute

Deretter regner Supplikant og AS ut sesjonsnøkkel (PMK) som senere brukes for å avlede temporære nøkler (PTK) til bruk i kryptering i CCMP/TKIP.

6. EAP Request/EAP-TLS

AS sender resten av sine meldinger i en enkel EAP request; Change Cipher Spec til det de har blitt enige om og TLS Finished handshake. Sesjonen som startet med ServerHelloDone avsluttes.

EAP Response/EAP-TLS

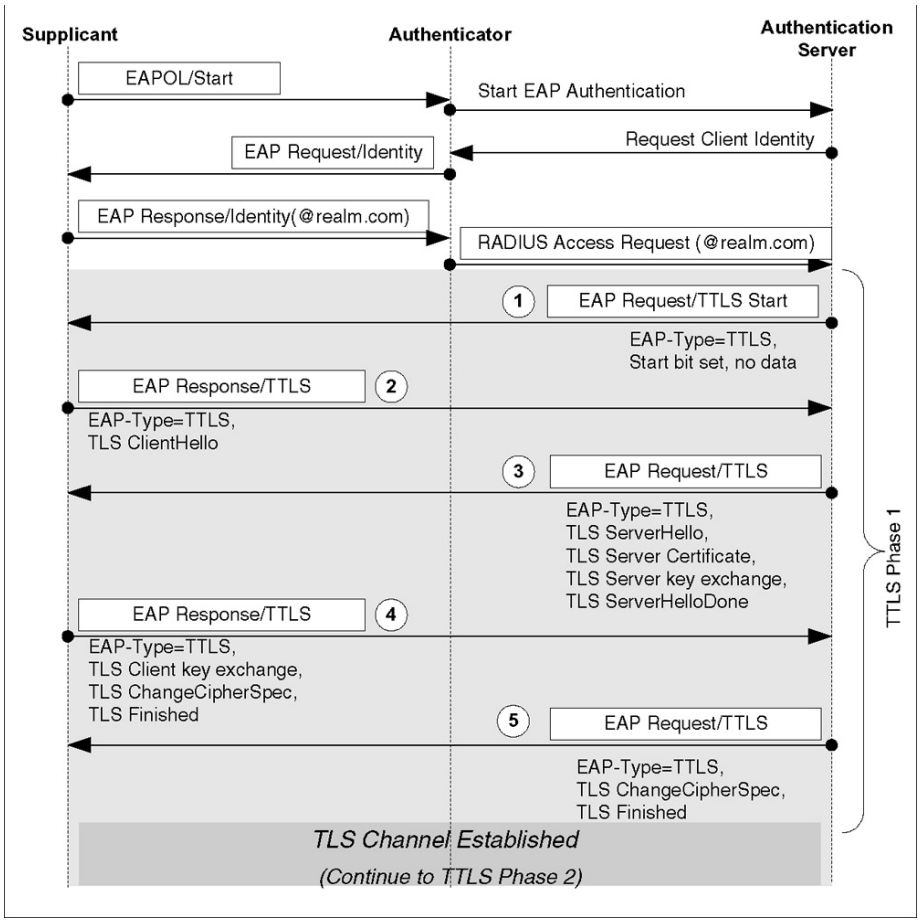
Avslutningsvis sender supplikanten en tom respons melding

EAP Success/RADIUS Access Success

AS sender EAP Success og overleverer sesjons-nøkler til autentikator (AP)

4.14.2. EAP-TTLS/MSCHAPv2

Metoden går ut på å etablere en kryptert TLS-tunnel i fase 1, for deretter å kunne bruke denne til å oversende autentiseringsdata via den mindre sikre MSCHAPv2 protokollen inne i denne. Det er verdt å merke seg at vi her beskriver TTLS version 0 [FUN], som er standarden Wi-Fi sertifiserer etter. Senere har det, uten at Wi-Fi har endret sine krav, kommet i en versjon 1, som har en del forbedringer, blant annet beskytter den mot man-in-the-middle angrep.



Figur 31 TTLS-fase 1 [HAR]

Før selve EAP-TTLS utvekslingen begynner kobler STA seg mot AP. Deretter sender klienten en anonym identititet til AS i svaret på AS sin request, slik:

Request Dette er starten på EAP utvekslingen. AS ber om identiteten til klienten
Response Her sender klienten en melding med en anonym identitet til AS

1 EAP Request/TTLS Start

AS sender en tom EAP-TLS request med start bit satt. EAP-Type er satt til EAP-TTLS

2 EAP Response/TTLS

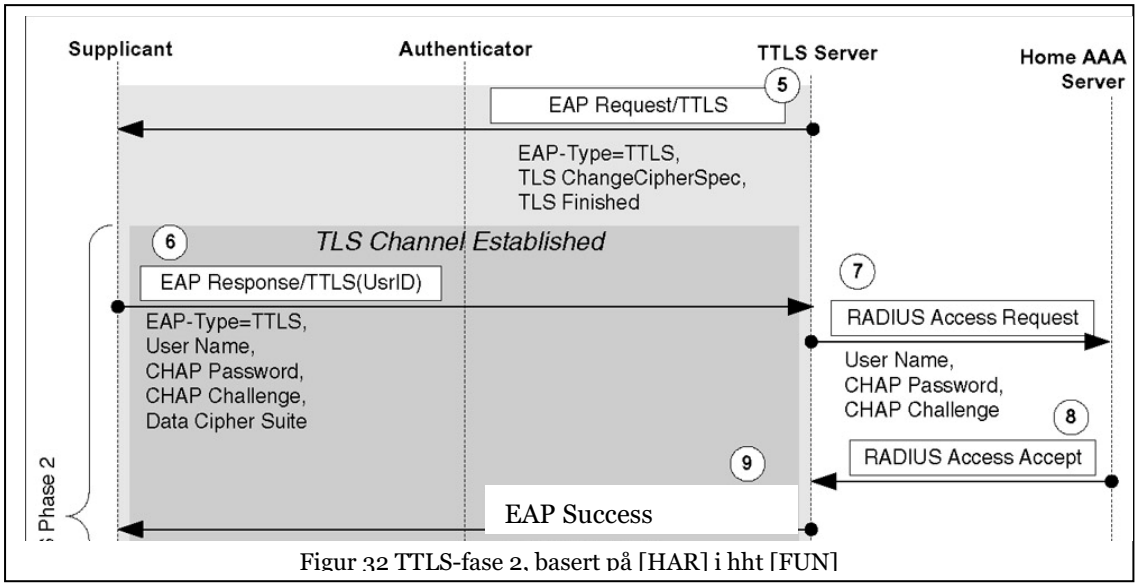
Supplikanten sender Client Hello med den samme informasjon som for en ordinær TLS-pakke. Dvs supplikantens TLS versjonsnummer, sesjons ID, et nonce, og hvilke cipher suites den støtter.

3 EAP Request/TTLS

AS sender to eller tre TLS meldinger i en enkel request. Server hello, AS Server sertifikat, og Server HelloDone.

4 EAP Response/TTLS

Supplikant svarer med flere TLS meldinger i en respons, nøkkelutvekslings parametre, utregning og oversending av pre-master secret (kryptert med AS sin offentlige nøkkel).



Figur 32 TTLS-fase 2, basert på [HAR] i hht [FUN]

5. EAP Request/TTLS

AS sender resten av sine meldinger i en enkel EAP request; Change Cipher Spec til det de har blitt enige om og TLS Finished handshake.

6. EAP Response/TTLS(UsrID) og RADIUS Access Request

Inne i den krypterte tunnelen kan nå supplikanten benytte den mindre sikre MS-CHAPv2 autentiseringen, og sender her sitt virkelige brukernavn og passord samt challenge til server

7.EAP Success/RADIUS Access Success
AS sender EAP Success og overleverer sesjons-nøkler til autentikator (AP)

Avslutningsvis regner Supplikant og AS ut nøkler som senere brukes til i CCMP/TKIP for å beskytte datakommunikasjonenen konfidensialitet og integritet.

4.14.3. EAP-PEAP

I likhet med EAP-TTLS går også denne metoden, beskrevet i [JOS], ut på å etablere en kryptert tunnel, for deretter å kunne bruke andre autentiseringsprotokoller inne i denne. Eksempler på dette er PPP Authentication Protocols (PAP), PPP Challenge Handshake Authentication Protocol (CHAP), Microsoft PPP CHAP Extensions (MS-CHAP), Microsoft PPP CHAP Extensions Version 2 (MS-CHAP-V2), Generic Token Card (GTC).

Wi-Fi alliance har imidlertid kun krav om MS-CHAP-V2 [RFC2749] og EAP-GTC, som er en del av [RFC3748] som indre protokoll.

Foruten å definere disse, har også Wi-Fi alliance spesifisert at PEAP versjon 0 skal brukes for MS-CHAP-V2 og at PEAP versjon 1 skal brukes for GTC. Det ser ikke ut til å eksistere større forskjeller mellom disse utover at Microsoft ønsker versjon 0 og RSA/Cisco støtter versjon 1. Som en konsekvens av dette så støtter Windows sin innebygde supplikant kun versjon 0.

PEAP autentiseringsprossess foregår også i to trinn, , og er eller svært lik EAP-TTLS hvor man først setter opp en kryptert TLS-tunnel og deretter tunnelerer enklere passordbaserte metoder basert på MS-CHAP eller GTC autentiseringsdata på innsiden

Mens MSCHAPv2 benytter brukernavn og passord fungerer GTC tilsvarende, men baserer seg på to-faktor autentisering. Passordet består av pin-kode pluss et tall generert fra GTC-tokenet.

4.14.4. LEAP

LEAP er en proprietær protokoll fra Cisco Systems. Dens utbredelse gjør at vi allikevel kort beskriver denne her. LEAP er en to-veis challenge response protokoll[40] som baserer seg på hemmelige, delte nøkler mellom supplikant og AS. Nøkkelen trenger ikke være kjent for AP. Det kreves eksplisitt støtte for LEAP i tillegg til generisk 802.1X-støtte

1. AS sender en tilfeldig challenge til klient
2. Klient beregner og returnerer response sammen med challenge til server
3. AS beregner og returnerer response

[40] Egentlig LEAP Challenge/Response som er modifisert MS-CHAPv2 [WRI03]

4. AS genererer og sender sesjonsnøkkel til AP sammen med EAP success-RADIUS
5. AP sender EAPOL-suksess melding.
6. AP genererer kopi av sesjonsnøkkel
7. AP sender en EAPOL-key notification melding for å aktivere kryptering.

Meldingene går ukryptert og metoden baserer seg på Challenge Response som i MS-CHAPv2. Metoden skiller seg klart fra de to andre tunneleringsprotokollene, EAP-TTLS og PEAP ved at autentiseringsdataene ikke er beskyttet av en kryptert tunnel under overføring.

4.14.5. Sammenligning sentrale egenskaper

I valg av metode vil også praktiske ting som spiller inn. Eksempler på dette vil være metodens kompleksitet, som hvordan nodene autentiseres og eventuelle krav som stilles til utstyret som skal delta i kommunikasjonen. Majoriteten av dette er behandlet i 4.14.1-4.14.4, men for oversiktens skyld fremstilles det her tabellarisk.

	EAP-TLS	**TTLS-MSCHAPv2**	**PEAPv1-GTC**	**PEAPv0-MSCHAPv2**	**LEAP**
Serverautentisering	Sertifikat	Sertifikat	Sertifikat	Sertifikat	Passord
Klientautentisering	Sertifikat	Passord	PIN+OTP	Passord	Passord
Supplikant Win	Integrert	3dje part	3dje part	Integrert	3dje part
Krav til KlientHW	Evt kortleser	Intet	Token	Intet	Intet
Indre autentisering	n/a	MSCHAPv2	GTC	MSCHAPv2	n/a
Krav til AS	RADIUS	RADIUS	RADIUS	RADIUS	RADIUS
Kildekode	Åpen	Åpen	Åpen	Proprietær	Proprietær
Mulig 2 faktor	Ja	Nei	Ja	Nei	Nei

Tabell 4 Sammenligning av EAP-metoder

4.14.6. Samsvar med RFC 4017

IEEE har overlatt til IETF å beskrive sikkerhetskravene for metoder som kan kan påberope seg å være i samsvar med "IEEE 802.11 EAP method requirements for wireless LANs". Kravene er beskrevet i [RFC4017] som opererer med 3 ulike nivåer, hvor *obligatorisk*, i motsetning til *anbefalt,* er nødvendig for å være i samsvar. *Opsjon* har mer fokus på funksjonalitet enn sikkerhet og er ikke vesentlig i vår kontekst.

Obligatorisk

Dynamisk nøkkelgenerering

EAP-metodens mulighet til å avlede nøkkelmateriale som Master Session Key (MSK). MSK skal kun brukes for å videre avledning av nøkkelmateriale og ikke for direkte beskyttelse av EAP-kommunikasjonen. Kan oversettes med dynamiske nøklergenerering.

Nøkkelstyrke>128bits

EAP-metoden må være kunne generere nøkkelmateriale med en effektiv nøkkelstyrke på 128bits.

Gjensidig autentisering

Partene i en EAP-utveksling må være i stand til å autentisere hverandre begge veier

Felles attributter (shared state equivalence)
Partene EAP-metoden må være i stand til tilgjensidig å enes om felles ”state”. Dette inkluderer, men begrenser seg ikke til, metodens versjonsnummer, autentiseringsdata, kryptografiske nøkler og valg av krypteringsalgoritme. Partene må enes om hva som skal holdes hemmelig dem i mellom og hva som kan gå i klartekst, herunder erverv av hverandres identitet (dersom denne er tilgjengelig)

Ordlisteangrep resistans

Motstandsdyktighet mot ordlisteangrep

MiTM resistens

Motstandsdyktighet mot man-in-the-middle angrep.

Beskyttede forhandlinger av sikkerhetsprotokoll

Dersom metoden forhandler sikkerhetsprotokoll for å beskytte EAP-forhandlingene må denne integritetsbeskyttes.

Anbefalt

Fragmentering
Metoden bør støtte fragmentering og defragementering hvis EAP-pakkene har mulighet til å overskride MTU på 1020 oktetter.

Skjuling av klient ID

Meldinger i EAP utvekslingen som inneholder partenes identitet bør konfidensialitetsbeskyttes.

Opsjon

Channel binding
EAP-metoden bør støtte en mekanisme som kan overbringe integritetsbeskyttede data, som endepunkt-identifikasjon til ”out-of-band” enheter.

Fast reconnect
Dersom en secutity association (SA) må reetableres bør dette gjøres med et redusert antall meldingsutvekslinger (sammenlignet med initiell etablering)

	EAP-TLS	TTLS-MSCHAPv2	PEAPv1-GTC	PEAPv0-MSCHAPv2	LEAP
Obligatorisk					
Dynamisk nøkkelgenerering	Ja	Ja	Ja	Ja	Ja
Nøkkelstyrke>128	Ja	Ja	Ja	Ja	Nei
Gjensidig autentisering	Ja	Ja	Ja	Ja	Ja
Felles attributter	Ja	Ja	Ja	Ja	Ja
Ordlisteangrep resistans	Ja	Ja	Ja	Ja	Nei
MiTM resistans	Ja	IA[41]	IA	IA	Ja
Beskyttede forhandlinger	Ja	Ja	Ja	Ja	Ja
Anbefalt					
Fragmentering	Ja	Ja	Ja	Ja	Ja
Skjult klient ID	Nei	Ja	Ja	Ja	Nei
Opsjon					
Channel binding	Ja	Opsjon	IA	IA	Ja
Fast reconnect	IA	Ja	Ja	Ja	Ja

Tabell 5 Samsvar med RFC 4017

Tabell 5 bygger på sammenstilling av funn i litteraturen, hovedsakelig basert på [NIST800-97],[VAC],[DAN] og viser hvordvidt metodene oppfyller sikkerhetskravene i RFC4017. Som det går frem av tabellen er majoriteten av metodene i samsvar med alle de obligatoriske kravene. LEAP skiller seg ut med manglende nøkkelstyrke og motstandsdyktighet mot ordlisteangrep. EAP-TLS skiller seg ut ved at den ikke er kjent for å være sårbar for man-in-the-middle anrep. PEAP og TTLS kan være sårbare mot dette dersom ikke spesielle forholdsregler taes. Se 4.14.8.

Motstandsdyktighet mot tradisjonelle angrep

Vi har også gjort en vurdering av metodenes motstandsdyktighet mot mer tradisjonelle angrep. Semmenstillingen er vist i Tabell 6. Resonnementene bygger på diskusjon av angrep i 4.14.7-4.14.9

	EAP-TLS	TTLS-MSCHAPv2	PEAPv1-GTC	PEAPv0-MSCHAPv2	LEAP
Protokollsikkerhet	God	Middels	Middels	Middels	Dårlig
Tapt passord	n/a	Dårlig	God	Dårlig	Dårlig
Tapt maskin	Middels	Dårlig	God	Dårlig	Dårlig

Tabell 6 EAP metodenes motstandsdyktighet mot tradisjonelle angrep

Skala: God, Middels, dårlig

4.14.7. Angrep mot LEAP

Asleap er et verktøy for ordliste angrep mot LEAP. Verktøyet ble gjort tilgjengelig på Defcon i 2004 [WRI03] . Asleap kan knekke passord enten i sanntid, eller kjøres som et offline angrep mot en bitstrøm som er spilt inn til lagringsmedium.

[41] IA – Implementasjonsavhengig. For MiTM-resistens se 4.14.8

Angrepet baserer seg blant annet på flere designmessige svakheter som LEAP arvet fra MS-CHAPv2. Eksempler på dette er brukernavn sendes i klartekst, samt at salt ikke brukes i det hashede passordet (MD4 NT Hash). Dette er egenskaper som gjør det enkelt å forberede og montere ordliste-angrep,

Tiltak

Cisco anbefaler enten et langt sterkt passord eller migrering til EAP-FAST, Cisco System sin proprietære arvtager etter LEAP. Nyere Cisco utstyr støtter dessuten EAP-TLS og tunnelerte protokoller som PEAP og TTLS.

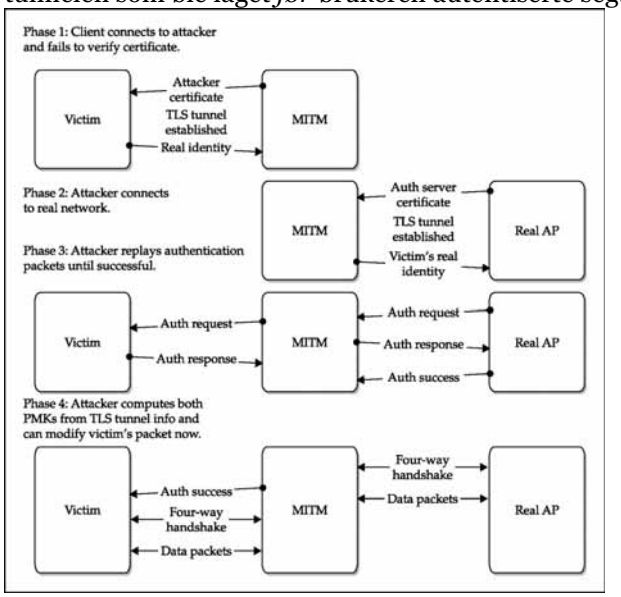
Problemet med sterke passord er at de er umulige for vanlige mennesker å håndtere[OU1]. Rapporten hevder også at 99% av alle passord i en organisasjon blir knekt i løpet av timer, og dessuten vil krav til sterke passord føre til at brukerne skriver disse ned. LEAP er derfor, i følge [OU1], et svært dårlig valg, særlig når det finnes løsninger som er langt mer robuste og ikke proprietære.

4.14.8. Angrep mot TTLS og PEAP

Både TTLS og PEAP er sårbare for Man-in-the-middle angrep. Dette gjelder uavhengig av om man benytter MSCHAPv2 eller GTC som indre protokoll. En potensielle sårbarhet spesifikk for MSCHAPv2 er caching av passord. Det er derfor hensiktsmessig å behandle disse hver for seg.

Angrep mot TTLS og PEAP generelt

TTLS og PEAP i versjonene som er godkjent av Wi-Fi-alliance er sårbare for Man-in-the-middle angrep. Sikkerhetsprotokollens natur med autentisering på innsiden av en allerede etablert kryptert tunnel er det som mulig gjør dette angrepet.
Ved bruk av PEAP/TTLS blir PMK til bruk i 4-way handshake senere avledet fra tunnelen som ble laget *før* brukeren autentiserte seg. Det er dette som utnyttes.



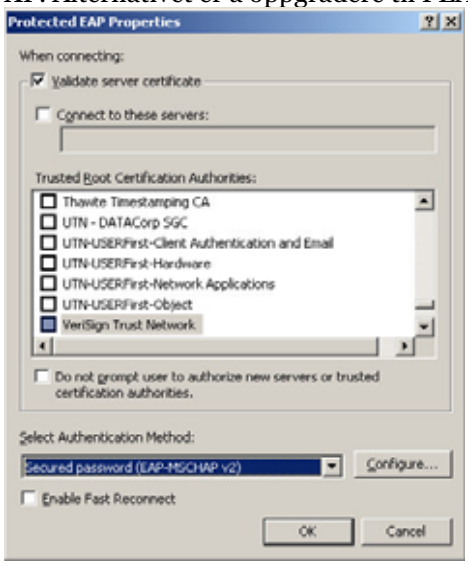
Figur 33 Man-in-the-middle angrep [CAC]

Hvis klienten ikke validerer server-sertifikatet, kan en ondsinnet sette opp et angrep som vist over. Et man-in-the-middle angrep. Han vil da opptre som et relè mellom

klient og AP og vil da potensielt kunne avlytte og/eller endre kommunikasjonen mellom STA og AP.

Tiltak

Man kan sikre seg mot denne typen angrep ved å sørge for at supplikanten er satt opp til å validere server sertifikatet [CAC]. I Windows gjøres dette ved å krysse av for *Validate server certificate* som vist i Figur 34 Validering av serversertifikat i Windows XP. Alternativet er å oppgradere til PEAPv2 og TTLSv1 når disse blir tilgjengelig.



Figur 34 Validering av serversertifikat i Windows XP

I et Windows-domene er det mulig å tvinge denne innstillingen på brukerne ved hjelp av såkalte gruppe policyer i (Group Policy Objects – GPO-er). Dette er standard verktøy i et Windows-domenemiljø.

Angrep mot MSCHAPv2

Problemet er av mer tradisjonell karakter, og bygger på det faktum at dersom enheten tapes vil uvedkommende enkelt kunne komme til autentiseringsdataene. By design cacher Microsoft Windows XP supplikanten passordet som benyttes for PEAP[42].

Et MSCHAPv2 passord er i praksis et Windows NTLM-passord som i sin natur er usaltet[43]. Når dette i tillegg blir liggende i registeret som en enkel MD4-hash uten bruk av salt, åpner dette for misbruk. Med tilgang til enheten vil det være mulig å knekke dette passordet ved hjelp et ordlisteangrep.

[42] Vi har ikke funnet det bevist at den TTLS-baserte MSCHAPv2 løsningen faktisk mellomlagrer passordet som en knekkbar hash på harddisk, men det vil uansett kunne være mulig til å finne spor av et slik når man tilbyr ”sømløs” login.

[43] Salt: ”Tilfeldige” bits som legges til passordstrengen for å gjøre ordliste angrep langt vanskeligere

Det er ikke mulig å fjerne dette valget med mindre man aktivt sletter en registernøkkel[44] i registry.

Eller sagt med Microsofts egne ord:
"When you successfully log on to a network that uses PEAP authentication, your credentials are automatically stored in the computer for re-use. For example, when you shut down and then restart your computer, you are automatically logged on to the wireless network. There is no option that you can configure in Windows XP to prevent the operating system from storing your credentials. By design, the cached credentials are not deleted and do not time out unless the user fails to authenticate or the wireless network is removed from the preferred list. However, you can delete the registry key where your user credentials are stored. When you do so, you are prompted to enter your credentials the next time you log on to the network" [KB823731]

Metoden for å endre i registeret garanteres heller ikke av Microsoft, da følgende advarsel ledsager beskrivelsen av hvordan slette registernøkkelen:

"Warning Serious problems might occur if you modify the registry incorrectly by using Registry Editor or by using another method. These problems might require that you reinstall your operating system. Microsoft cannot guarantee that these problems can be solved. Modify the registry at your own risk".

Det er interessant å merke seg at artikkelen[KB823731] ble opprettet så sent som 21 mai 2007.

Tiltak
Kryptere hele eller deler av harddisken hvor passord-hashen ligger. Bruke sterke passord. Ha rutiner for sperring av brukerkonti eller endring av passord for brukere som har tapt enheter. Sørge for å slette registernøkkelen automatisk etter bruk. For eksempel med et avloggingsskript. Vurdere å bytte til to-faktor løsning.

Andre angrep
Angrep av mer marginal interesse er at det er en teoretisk sannsynlighet for supplikanten faktisk sender sin egentlige identitet før TLS-tunnelen er satt opp. Imidlertid skal identiteten være feilaktig (bogus) eller anonym

4.14.9. Angrep mot EAP-TLS

Å angripe EAP-TLS regnes som svært vanskelig. Et vellykket kryptografisk angrep vil sannsynligvis være ekvivalent med at sikkerheten i RSA er brutt. I en risikoanalyse vil sannsynligheten for dette være tilnærmet ikke-eksisterende. Angrep mot EAP-TLS vil da antas å være av mer praktisk karakter, og rettet mot oppbevaringen av den private nøkkelen. Dersom denne ligger på en dårlig beskyttet PC vil det være mulig å få tak i denne. Et vellykket angrep krever også at man får tak i brukerens sertifikat, noe som bør være mulig ettersom man har fått tak i den private nøkkelen. Angrepet gjennomføres helt enkelt ved å autentisere som brukeren man har stjålet autentiseringsakkreditivene fra, og tilgang til nettverket gis som denne brukeren, med de rettighetene denne har. Identitetstyveriet skaffer ikke uten videre tilgang til å

[44] HKEY_CURRENT_USER\Software\Microsoft\Eapol\UserEapInfo.

avlytte annen trådløs trafikk ettersom de har andre PMK. Da vil evt løsningen være å ARP-spoofe dem og gjennomføre et MiTM angrep.

Tiltak

Et praktisk forsvarstiltak vil være å kryptere hele eller deler av harddisken på den trådløse enheten. Alternativet er å oppbevare sertifkatet eller den private nøkkelen på et smartkort eller lignende medium og beskytte dette med av en PIN-kode. Dersom dette gjøre regnes et vellykket angrep mot EAP-TLS som nærmest umulig. [CAC]

4.14.10. Angrep mot WPA-PSK

PSK er Preshared Key som man benytter når RADIUS infrastruktur ikke er på plass., og systemet autentiserer ikke brukeren, men enheten som nøkkelen ligger på. Dette innebærer at den vil ha alle praktiske svakheter som er forbundet med nøkkeladministrasjon av statiske nøkler. Mye av denne problematikken er allerede drøtet i 4.6ff.

Det er kjent at WPA-PSK ordliste angrep er effektivt ettersom SSID er en del av nøkkelen[CAC]. Ettersom SSID går i klartekst, og er en del av nøkkelen vil denne gi verdifull til angriper. Ordliste-angrep kan kjøres svært effektivt dersom hash-tabeller er generert på forhånd, eller ved å benytte slik allerede tilgjengelige[45] tabeller. Selv om SSID er kjent vil det ta lang tid å generere opp nye hash-tabeller dersom SSID unik.

[802.11i] har følgende betraktninger om metoden: Preshared Key består av 256 bits eller 64 oktetter når representert Heksadesimalt. Standarden slår fast at det er vanskelig for brukerne å taste inn 64 hex karakterer. Et passord/passphrase har typisk en relativt lav sikkerhet og anbefales bare hvis det upraktisk å bruke en sterkere form for autentisering. En nøkkel som genereres av et passord som er mindre enn cirka 20 karakterer vil lite trolig kunne motstå et ordliste angrep [802.11i].

Angrepsverktøy finnes, for eksempel CoWPAtty. Se ellers Appendiks A for verktøy.

Tiltak

Kryptere hele eller deler av harddisken hvor WPA-PSK nøkkelen ligger. Endre SSID fra det som er standard fra leverandør. Bruke sterke passord.

4.14.11. Angrep mot RADIUS

RADIUS har flere svakheter som må adresseres. Denne knyttes i hovedsak til kommunikasjon mellom AP og RADIUS.

Kort oppsummert består problemet i at trafikken er sårbar for en rekke aktive og passive angrep, men da som tradisjonelle angrep på et kablet nettverk. Eksempler på dette er avlytting, endring av pakker under transport, ordlisteangrep mot shared secret, replay. For å kunne utnytte de kjente svakhetene knyttet til RADIUS-kommunikasjon kreves det en form for tilstedværelse på det kablede nettet mellom RADIUS og AP.

Problemene er utførlig beskrevet i [BRO]2.4, [HAR] 2.6.3, og [RFC3579], [RFC2607], [RFC 2865], [RFC3162] og det henvises videre til disse kildene.

[45] Typisk tilgjengelig som såkalte rainbow tables på internett.

Tiltak

Kryptere kommunikasjon mellom AP og AS med IPSec [RFC2401]. Et minimum er en meget kompleks shared secret. [RFC3579] anbefaler bruk av IPSec.

4.14.12. Fremtidige EAP-løsninger

PEAPv2 og TTLSv1 støtter kryptografisk binding mellom indre og ytre protokoll og vil således være reistent mot MiTM angrep.

EAP-TLS i ny versjon er egentlig EAP-PEAP-TLS sørger for beskyttelse av identitiet, noe som er et problem i EAP-TLS. Metoden er allerede i dag støttet i Windows XP supplikant, men er utenfor standardene til Wi-Fi alliance. Det finnes dermed ingen garanti for at dette er støttet i aksesspunktene eller i andre supplikanter på andre plattformer.

4.15. Kostnader med de ulike metoder

De ulike metodene for kryptering og autentisering har naturlig nok en kostnadsside, økonomisk og administrativt. For oversiktens skyld drøfter vi kortfattet noen av disse her.

4.15.1. Kryptering

I et Windows-miljø er TKIP støttet som standard fra service pack 1. Interessant nok er det ikke støtte for WPA2, dvs CCMP i Windows XP. Dette gjelder også dersom man har alle programvareoppdateringer som tilbys gjennom den automatiske oppdateringstjenesten[46] som Microsoft tilbyr.

Da denne oppgaven ble påbegynt var det et krav at man måtte installere et tillegg for å få CCMP/WPA2-støtte; nemlig hurtigfiksen [KB893357]. De nevnte programvareoppdateringene er gratis tilgjengelig for lisensierte versjoner av Windows.

I august 2007 ble det imidlertid sluppet en ny hurtigfiks [KB917021]. I tillegg til CCMP-støtte, beskytter denne hurtigfiksen også mot cloaking angrep. Metoden den gjør dette på er at den sørger for at klienten ikke kringkaster sin liste over fortrukne nettverk, dersom disse ikke er innen rekkevidde

4.15.2. Autentisering

Det er opplagt, og stadig referert i litteraturen, at det å rulle ut en full PKI-infrastruktur har en kostnadsside både økonomisk- og administrasjonsmessig [VAC]m.fl. EAP-TLS faller innenfor denne kategorien. Det kreves både server- og klient-sertifikater enten disse legges på selve supplikanten eller på et smartkort. Dersom sistnevnte velges krever dette både innkjøp og vedlikehold av selve smartkortet og evt kortlesere.

Det tilsvarende gjelder for OTP-løsninger. Disse genererer både initielle- og vedlikeholdskostnader. Kostnadssiden vil være knyttet til innkjøp og vedlikehold av selve tokenet som alle brukernes må ha, og en server hvor løsningen er installert. Ofte er denne sammenfallende med RADIUS-serveren. PEAP-GTC faller innefor denne

[46] "Windows Update"

kategorien. Ettersom GTC kun er støttet i versjon 1 av PEAP, vil dette også innebære at man må ha en tredje parts supplikant på Windows klienter.

Valg av en LEAP eller EAP-TTLS løsning i et Windows miljø krever tredjeparts autentiseringsserver og supplikanter, med de direkte økonomiske- og administrative kostnader dette medfører.

Alle metoder, unntatt LEAP, vil gi kostnader og administrasjon rundt å anskaffe og vedlikeholde et offisielt sertifkat fra en godkjent Certfikate Authority (CA), kostnadene er imidlertid av marginal karakter i en slik implementasjon. Dessuten vil det sannsynligvis være mest hensiktsmessig å benytte en intern CA.

5. Konklusjon teoristudium

Etter analysene av de ulike protokollenes godhet foreslår vi nå en rangering av metoder. Ettersom Microsoft Windows er det suverent mest utbredte operativsystemet på klienter vil dette bli diskutert som en faktor man må ta hensyn til.

5.1. Rangering kryptering

WEP er grunnleggende kompromittert på designmessig og kryptografisk nivå og er, uavhengig av nøkkellengde, ikke anbefalt. Ettersom TKIP bygger på WEP, og i praksis adresserer alle kjente svakheter pr dags dato, så er den allikevel bygd på WEP og RC4. MICHAEL eller også kjent for å være en relativt svak integritetsalgoritme. Det vil være sannsynlig [VLA] at angrep på denne vil lykkes i nær fremtid, ref for eksempel arbeidet til [HOL]. Konsekvensen av et brudd i TKIP vil føre til fullt brudd på sikkerhetsprotokollen. TKIP er altså designet etter prinsippet som ofte omtales som ”penetrate-and-patch”, dvs sårbarheter avdekkes og så fikser man disse etter at disse er oppdaget. Denne designfilosofien frarådes av autoriteter [VIE]. CCMP på sin side er designet fra bunn med bruk av anerkjente algoritmer for konfidensialitet og integritet. Prinsippet kalles gjerne ”secure by design”.

Dersom Windows XP er valgt operativsystem på STA kreves det installasjon av hurtigfiksen [KB917021].

Metoder for konfidensialitet og integritet rangert etter godhet; Beste først

1. CCMP
2. TKIP
3. WEP

5.2. Rangering autentisering

Tradisjonell litteratur som omhandler autentisering i trådbaserte LAN anbefaler bruk av to-faktor autentisering, og da særlig for autentisering fra et fremmed nett, for eksempel for fjerntilgang over internett. Interessant nok er dette overhodet ikke fokus i litteraturen som beskriver og drøfter sikkerhet i WLAN. Dette kan ha en sammenheng med at man i en årrekke har hatt fokus på å gjøre selve protokollene sikrere.

Svært mange fremholder EAP-TLS som autentiseringsmetoden med best sikkerhet, men i motsetning til litteraturen for autentisering i tradisjonelle LAN unnlater man å gjøre rede for at sertifikatet bør oppbevares på et eksternt medium for eksempel et smartkort.

EAP-TLS er imidlertid basert på full PKI-infrastruktur med sertifikater både på supplikant og AS. PKI er tradisjonelt tungt og implementere i en organisasjon dersom en slik ikke allerede er på plass. Metoden tilbyr svært god protokollsikkerhet. Imidlertid er tap av bærbare enheter et så stort problem at kravet til to-faktor autentisering i vår kontekst må veie tyngre. Dette betinger selvsagt at utforming av de to faktorene inviterer til at den fysiske enheten holdes atskilt fra tokenet i en GTC-basert metode, og at smartkortet som brukes i EAP-TLS oppbevares et annet sted enn i

enhetens kortleser. EAP-TLS er innebygget i supplikanten til Windows XP og senere. Dette er ikke tilfelle for PEAP-GTC. Sistnevnt krever tredjeparts supplikant.

På tross av at PEAP i dagens versjon er sårbar for man-in-the-middle angrep, så er det relativt greit å sikre seg mot denne type angrep ved en kombinasjon av å tvinge supplikantene til å validere server sertifikatet og deteksjons- og jammesystemer mot uautorisert trådløse aksesspunkter. Denne funksjonen tilbys av alle større leverandører av trådløse nettverksløsninger.

Vi er av den klare oppfatning av at sannsynligheten og konsekvensen av å miste et passord utgjør totalt sette en større risiko enn risikoen for man in the middle angrep.

Det finnes altså to metoder for å benytte passordene som allerede er i bruk i virksomhetens brukerdatabase, nemlig ved bruk av MS-CHAPv2, inne i TTLS eller PEAP. TTLS og PEAP skiller seg fra hverandre ved at TTLS krever en kommersiell tredjeparts supplikant, som tradisjonelt er priset både for investerings- og årlige vedlikeholdskostnader.

Supplikant som støtter PEAP metoden er på sin side inkludert i operativsystemet Microsoft Windows XP og Vista. Imidlertid har metoden en ikke ubetydelig sårbarhet i og med at brukerens påloggingspassord som standard lagres i registry på Windows maskinen. WPA-PSK og LEAP-metoden er bevist sårbare for ordliste angrep. WEP har enorme mangler og kompromitteres nå på under 60 sekunder. Kun lavnivå metoder som MAC-adressefilter er mindre egnet for å ivareta sikkerheten enn WEP, da disse metodene kun trenger et passivt angrep for at autentiseringsakkreditivet kan avsløres.

Metoder for autentisering blir da slik, rangert etter godhet; Beste først

- EAP-TLS m/sertifikat på eksternt medium
- PEAPv1/EAP-GTC
- EAP-TLS
- EAP-TTLSv1-MSCHAPv2
- PEAPv0-MSCHAPv2
- LEAP
- WPA-PSK
- WEP
- Lavnivå-tiltak

5.2.1. Valg av metode – noen praktiske betraktninger

For å kunne velge metode er det åpenbart at man må gjøre en kost/nytte analyse og se dette opp mot flere faktorer, som for eksempel sikkerhetspolicyer, risikoanalyser og trusselbildet generelt.

Det vil variere hva slags behov ulike virksomheter har, men det vil være hensiktsmessig å se på hva man allerede har av infrastruktur i virksomheten. RADIUS-server er imidlertid noe som klart anbefales, og som har en marginal kostnad. En overordnet anbefaling kan være at man forsøker å gjenbruke infrastruktur som allerede er i virksomheten. Hvis man allerede benytter Smartkort og PKI-infrastruktur vil det være naturlig å bruke denne. Tilsvarende vil det være at dersom

en OTP-løsning benyttes for fjerntilgang vil det være naturlig å gjenbruke også for WLAN. Dersom det ikke er krav til to-faktor må man vurdere om man vil ta de ulike kostnadene med å rulle ut PKI-infrastruktur og se dette opp mot sikkerhetsnivået som kreves, fordelen her som med PEPv0-MSCHAPv2 løsningen er at man slipper tredjeparts supplikanter.

Av løsningene for beskyttelse av konfidensialitet og integritet er det CCMP og TKIP som er aktuelle. Som beskrevet er det fra et sikkerhetsmessig ståsted i øyeblikket ingen kjente praktiske angrep mot noen av disse, slik at man må vurdere om man skal være rustet for fremtiden ved å ta den administrative og eventuelle direkte økonomiske kostnaden det er å få samtlige trådløse enhter opp med CCMP støtte.

6. Empirisk undersøkelse

Vi har valgt å gjennom føre 5 intervjuer for å operasjonalisere forskningsspørsmål 2 og 3 i 1.2

- Hvilke metoder for sikring av WLAN blir brukt av et utvalg virksomheter?
- Hvorfor har virksomheten valgt denne løsningen?

Det har blitt valgt ut fem virksomheter for å sjekke antakelsene vi hadde innledningsvis. Disse fem består av en av Norges største videregående skoler, en større høgskole med tre studiesteder, tre børsnoterte multinasjonale virksomheter hvor den minste har en årlig omsetning på 3 milliarder NOK. Samtlige intervjuobjekter oppgir at de har langt over 1000 brukere. På grunn av anonymiseringskravet gir vi for metodens del disse virksomhetene fiktive navn; navn som også sier hvilken bransje de hovedsakelig opererer innenfor. De fem er:

- Den Videregående Skolen (Vgs)
- Høgskolen
- Petroleumsvirksomheten
- Salgsvirksomheten
- Distribusjonsvirksomheten

Virksomhetene har egne IT-avdelinger, fire av disse har hovedsete i Norge, mens den femte har en IT-avdeling i Norge som fungerer som en autonom enhet.

Vi ønsket å finne ut hvilke metoder av aktuell WLAN-sikkerhet virksomhetene hadde rullet ut, og hvorfor de hadde valgt den aktuelle løsningen. Vi antok, etter at teoristudiet var gjennomført, at sammenlignet med våre funn så har ikke virksomhetene valgt den mest robuste løsningen for autentisering og sikring av integritet og konfidensialitet. Videre hadde vi en antakelse om virksomheten tror de har valgt den mest robuste løsningen, men at det i praksis var helt andre drivere som har blitt lagt til grunn for valg av løsning enn sikkerhet. Vi forventet også å finne at valgene var basert på anbefalinger fra produkt- eller tjeneste-leverandører, og at valget ikke samsvarer med hvordan virksomheten ellers behandler tilgang fra et eksternt nett.

Etter at intervjuene var gjennomført pekte resultatene entydig i retning av at valgene som i sin tid ble gjort, var basert på anbefalinger fra leverandører. Vi valgte derfor å kontakte 3 leverandører for å finne ut hvilke løsninger de anbefaler i dag, og hvorfor. De ble valgt ut 2 ledende WLAN-produsenter med egne tekniske konsulentavdelinger, og ett anerkjent konsulentselskap som yter konsulentbistand, samt designer og leverer løsninger basert på markedsledende produsenter. Det er ikke gitt at disse leverandørene har gitt anbefalinger til våre intervjuobjekter.

6.1.Drøfting av funn

Ingen av virksomhetene tilbyr i dag full PKI-infrastruktur. For hjemmekontorløsninger benytter to av virksomhetene to-faktorautentisering basert på OTP, men dette er ikke tatt i bruk for autentisering i WLAN.

Alle virksomhetenes WLAN-løsning gir tilgang til ressurser som ellers bare er tilgjengelig fra det kablede nettverket i virksomhetens lokaler. 3 av 4 virksomheter som krever autentisering til WLAN tilbyr gjestenettverk som gir ren internett-aksess. Den fjerde har umiddelbare planer om en slik løsning. Samtlige løsninger er basert på en captive-portal hvor et temporært brukenavn og passord deles ut ved behov. To av disse tre sender autentiseringsdata i klartekst over http protokollen. Dersom ikke kryptering er ivaretatt på høyere lag, for eksempel ved hjelp av SSL eller SSH vil all datatrafikk gå i klartekst.

Samtlige virksomheter har basert sine valg av løsninger på anbefalinger fra leverandører, mens leverandørene på sin side har designet løsningsforslaget på bakgrunn av krav fra kundene. Kun èn av virksomhetene så ut til å ha sikkerhet som den primære driveren for valg av WLAN løsning, for øvrig den samme virksomheten som har reflektert over hvorvidt de har valgt den mest robuste løsningen. Deres konklusjon er at det har de ikke, og kommer til å oppgradere til en to-faktor løsning basert på EAP-TLS. De andre oppgir fortrinnsvis tillit til merkevaren, kompatibilitet og roaming som årsak for sitt valg.

Sammenlignet med den utarbeidede rangeringen har ingen valgt den beste løsningen for autentisering; 3 av virksomhetene benytter en RSN-løsning, og tunnelerer MS-CHAPv2 over PEAPv0, den minst robuste av Wi-Fi metodene som baserer seg på 802.1X. PEAP-metodene kan være sårbare for man-in-the-middle angrep, men dette kan elimineres ved at klienten validerer server-sertifikatet. Dette hadde 2 av virksomhetene gjort. En virksomhetene har dessuten vært nødt til å ta i bruk WPA-PSK på enkelte av enhetene. Dette innebærer at den totale sikkerheten på WLAN-et ikke vil være bedre enn dette.

Det var overraskende å finne at en av virksomhetene, Distributøren, et multinasjonalt selskap med et 20 talls milliarder i årlig omsetning ikke hadde sikret nettet sitt med annet enn henholdsvis MAC-adressefilter og WEP. En av virksomhetene, Høgskolen hadde valgt å ikke sikre nettverket sitt i det hele tatt, men valget begrunnes med at designet var tatt på bakgrunn av en risikoanalyse som har vært gjennomført.

Både Distributøren, Høgskolen og Salgsvirksomheten kommer til å oppgradere systemene sine i nær fremtid. Den overordnede årsaken er kravet til bedre sikkerhet.

6.2. Intervju i virksomheter

Sammendrag av intervjuene gjengis pr virksomhet gjengis nedenfor.

6.2.1. Den Videregående Skolen

2 Intervjuobjekter, begge førstekonsulenter med ansvar for trådløst nettverk.

Den Videregående Skolen(Vgs) tilbyr trådløs dekning på nær 100 % av sine 36 000 kvadratmeter. Løsningen er basert på 3Com WLAN-kontrollere tilknyttet ca 140 aksesspunkter og 2 radiusservere i klynge for redundans. Primær driver for valg av løsning var kravet fra skoleledelsen om å tilby en fleksibel løsning for å ivareta skolen gode renommè. Skolen tilbyr trådløs nettverkstilgang både for gjester og elever/ansatte. Tilgang til virksomhetsnettverket gis kun til elevnettet som befinner seg i et separat virtuelt LAN (VLAN). Det er ikke mulig å nå ressurser i ansattes VLAN.

Vgs. benytter to ulike aksessmetoder for å nå det trådløse nettet. Disse omtales internt som ”RADIUS-løsningen” og ”WPA-løsningen”. Begge metodene benytter TKIP for kryptering, noe som fylkeskommunen mente var ”sikkert nok” mens RADIUS-løsningen benytter PEAPv0-MS-CHAPv2, så benytter WPA-løsningen pre-shared key for autentisering.

Det benyttes selvgenerert sertfikat på RADIUS-server, uten godkjenning av sertfikat på supplikant.Det er ingen tiltak i forhold til bortkomne enheter, og ingen sikring av informasjon om passord i registeret på Windows arbeidsstasjoner.

RADIUS er en føring i fylkeskommunens sikkerhetspolicy for autentisering, mens WPA-løsningen ble opprettet som en følge av at det var nødvendig for å få login-skript til å fungere på klasserom og mobile klassesett av PC-er. Kompatbilitet.

RADIUS-server er plassert på et åpent VLAN og er tilgjengelig for alle. Det benyttes ikke kryptering mellom autentikator og RADIUS og det er ikke definert kompleksitetskrav på shared-secret. RADIUS server er satt opp til kun å kommunisere med WLAN-kontroller.

Det er ikke kompleksitetskrav eller krav til bytte av Preshared Key i WPA-løsningen.

Av andre relevante sikkerhetstiltak nevnes deteksjon av falske aksesspunkter, og mulighet til å sette disse ut av spill.

Det er ingen planer om å endre trådløst nettverksmiljø i nær fremtid.

For fjerntilgang benyttes samme brukernavn og passord som på lokalnettet og gir tilgang til elevenes hjemme- og fellesområde.

6.2.2. Petroleumsvirksomheten

2 intervjuobjekter, totalansvar for LAN/WAN løsninger i Petroleumsvirksomheten over hele verden.

Petroleumsvirksomheten (PV) tilbyr trådløs dekning, for potensielt 1200 bærbare enheter, på noen hundre kvadratmeter i fjortende etasje på hovedkontoret. I praksis er det i underkant av 250 samtidige brukere på Windows arbeidsstasjoner. Løsningen er basert på 2 Cisco WLAN-kontrollere i klynge med dedikert administrasjons-server fra samme produsent. PV benytter 2 Microsoft 2003 servere med Microsoft Internet Authentication Service (IAS) som RADIUS tjeneste, og har således redundans både på autentikator og AS. Primær driver for valg av løsning var krav om trådløs tilgang for

gjester, og at man har god erfaring med leverandør samt kravet om kompatibilitet med eksisterende Cisco nettverksutstyr og nærhet til kunnskap om systemet. Man har ingen planer om å utvide eller bytte ut noe på løsningen i nær fremtid. Dette er delvis basert på inkompatibilitet med tilgjengelige nettverkskort på mange av klientene, samt at dette vil medføre betydelige økonomiske investeringer. Tilgang fra trådløst virksomhetsnettverk gir tilgang til samtlige nettverksressurser ekvivalent med det kablede nettverket. Det vil blant annet si virksomhets- og kundedata.

PV benytter en mix av TKIP og CCMP for kryptering, hvor det er opp til supplikanten å velge. I praksis er det kun TKIP som benyttes. Krypteringsløsningen ble anbefalt og satt opp av leverandør. På autentiseringssiden benytter man PEAPv0-MS-CHAPv2 og begrunner dette med anbefaling fra leverandør.

RADIUS-server er plassert på LAN. Det benyttes ikke kryptering mellom autentikator og RADIUS og det er ikke definert kompleksitetskrav på shared-secret. RADIUS server er satt opp til kun å kommunisere med WLAN-kontroller.

Det benyttes selvgenerert sertfikat på RADIUS-server, med godkjenning av sertfikat på supplikant.Det er ingen tiltak i forhold til bortkomne enheter, men innholdet er kryptert. Passord må byttes hver 90. dag.

For fjerntilgang benyttes to-faktor autentisering med RSA SecurID OTP.

6.2.3. Salgsvirksomheten

Intervjuobjekt: IT-sjef

Salgsvirksomheten (SV) har tilbudt trådløs nettverkstilgang siden før 2005 i 4 av de totalt 12 landene hvor de er etablert. Dette fordeler seg på 93 aksesspunkter over 25 000 kvadratmeter. Løsningen er basert på 2 Cisco WLAN-kontrollere i klynge, og kommunikasjonen mellom disse og aksesspunktene er kryptert over MPLS.

Det tilbys trådløs nettverkstilgang for kontor-PC-er og håndholdte enheter på lageret. Designmessig er det lagt opp til at man får tilgang til terminalserver, e-post og kontorstøtteapplikasjoner over WLAN. Tilgang til for eksempel kundedata fordrer bruk av terminalserveren.

Hjemmekontor-løsningen baserer seg på bruk av to-faktorløsning fra RSA, med tilsending av kode til mobiltelefon. Denne i kombinasjon med brukernavn og PIN-kode gir tilgang til terminalserver og SSL-VPN for å aksessere virksomhetens ressurser på filnivå.

Primær driver for valg av WLAN-løsning var kravet til standardisering og kompatibilitet med eksisterende Cisco nettverkselektronikk. Forutsigbarhet og vissheten om at aktøren ville være i markedet i overskuelig fremtid var også avgjørende. Man er også av den oppfatning at Cisco leverer sikre løsninger med høy teknisk kvalitet, samt at det er god tilgang til kompetanse på produktene. Valget var basert på egen kunnskap i kombinasjon med anbefalinger fra leverandør.

Krypteringsløsningen som er valgt er utelukkende TKIP og autentisering foregår ved hjelp av PEAPv0-MS-CHAPv2.

En føring for valg av autentiserings- og krypteringsløsning i WLAN er at man er pålagt å være i samsvar med Payment Card Industry (PCI) Standarden, en omforent standard som berører alle kunder av de store kredittkortleverandørene. TKIP var i henhold til intervjuobjeket et minimum for kryptering, og en RADIUS-løsning et minimum for autentisering.

Andre faktorer som spilte inn på valget var egen definerte sikkerhetskrav, ytelse og kompatibilitet med håndholdte enheter som ikke støtter kraftigere kryptering enn TKIP.

AS tillates kun å kommunisere med predefinerte autentikatorer, det er krav til kompleksitet på shared secret og trafikken er kryptert med IPSec.

Dersom en bærbar enhet forsvinner sperres brukeren i systemet. Som standard krypteres diskene for mellomledere og oppover, man har passord-kompleksitetskrav og krever passordbytte hver 60.dag.

Man har dessuten mulighet til å oppdage og eliminere falske aksesspunkter fra kontroller. Det er dessuten tatt i bruk trådløse innbruddsdeteksjonssystemer (Wireless Intrusion Protection Systems (WIDS))

6.2.4. Distributøren

Intervjuobjekt: Konstituert IT-sjef

Distributøren er etablert i 3 land og virksomheten i Norge er en autonom enhet som har lokalt driftsansvar for alt annet enn perimetersikkerhet. Kontoret i Norge har i underkant av 150 ansatte, men tilbyr trådløs nettverksaksess for selskapets 2000 ansatte dersom disse er på kontoret. Løsningen er basert på aksesspunkter fra HP uten sentralisert administrasjon. Hvert aksesspunkt på konfigureres for seg.

Trådløs nettverksaksess tilbys på to ulike nivå. Et ”Warehouse-nett” for tilgang til kundesystem, plukklister osv for de ansatte på lager og distribusjon. Og et ”Hus-nett” for administrativt og salgspersonell for full tilgang på lik linje med det kablede LAN-et.

Man tilbyr fjerntilgang over en tradisjonell lag 3 VPN løsning fra Nortel, og som en reseverløsning er det mulig å benytte Microsofts innebygde PPTP tjeneste. Bakgrunnen er problemer med lag 3 VPN over enkelte ISP-er. Uten bruk av de nevnte krypteringsløsningene er det mulig å nå interne nettverksressurser gjennom terminalservere i DMZ. Dette har blitt etablert som en tjeneste da mange av virksomhetens selgere ofte befinner seg ute hos kunder som ikke tillater tunnelert trafikk over sine brannvegger.

Hus-nettet benytter seg av 104-bits WEP-kryptering, mens Warehouse-nettet er åpent, med MAC-adressefilter som eneste autentiseringsmekanisme.

I samråd med en leverandør, valgte man 104-bits WEP-kryptering på hus-nettet basert på en forståelse av at man ønsket en standardløsning, som er sikrere enn 40-bits. Det var også et krav til løsningen at den skulle være lett å rulle ut og implementere. I Warehouse-nettet er de trådløse enhetene med montert i trucker slik at kravet til roaming mellom AP-er er sentralt for en fungerende løsning. Disse enhetene fikk man ikke til å fungere med WEP, derfor ble MAC-adresse filter valgt. Kompatibilitet.

Dersom en bærbar enhet kommer bort sperrer man brukeren på nettverket.

Distributøren har planer om å bytte WLAN-miljø i nær fremtid. I en slik løsning vil man ha fokus på pris, dekning og roaming og sikkerhet. Intervjuobjektet sier sikkerhet i organisasjonen vil få større fokus i tiden fremover.

6.2.5. Høgskolen

Intervjuobjekt: IT-leder og tidligere IT-leder, nå avdelingsdirektør.

Høgskolen er etablert på 3 studiesteder med totalt i underkant av 3000 studenter og ansatte. De 3 studiestedene har tilbudt trådløs nettverkstilgang siden henholdsvis 2001, 2003 og 2007. Det opereres med 2 ulike nettverk pr studiested, et ansattnettverk og et studentnettverk.

Det tilbys hjemmekontor-løsning for tilgang til ansattnettet basert på tradisjonell lag 3 VPN, med sertifikater også på klienter.

Avhengig av studiested tilbys det mellom 90 og 100 % trådløs dekning, fordelt på totalt ca 30 000 kvadratmeter. Løsningen er basert på nettverksutstyr fra Cisco uten sentralisert administrasjon. Det gis trådløs tilgang til studentnettet for studenter, ansatte og gjester. Det ermulig å nå ansattnettverket gjennom å autentisere seg over VPN-løsningen som brukes også for hjemmekontorløsningen.

IT-leder kan opplyse om at de er ingen sikkerhet på det trådløse nettverket, utover at man skjuler SSID på det ene studiestedet, og har satt DHCP-lease time til 12 timer. I en periode hadde man også MAC-adressefilter på dette studiestedet, dette er imidlertid fjernet på grunn av administrativ overhead. Den overordnede årsaken til valg av løsning var basert på at høgskolesektoren hadde god erfaring med Cisco som leverandør. Valget ble fattet på bakgrunn av pris, krav til ytelse og egen kunnskap og anbefalinger fra leverandør og Uninett. I 2001 startet dessuten høgskolen opp ett nytt studietilbud som i sin natur krevde WLAN.

Den tidligere IT-lederen begrunner valget om å implementere et helt åpent system med at da WLAN ble utbygget på det første studiestedet i 2001 så man at eneste alternativ for sikring var WEP. Allerede på den tiden var sikkerheten i WEP brutt, og man så ingen sikkerhetsmessig oppside i å benytte denne.

Viktige momenter i valg av en åpen løsning begrunnes også med at høgskolesektoren tradisjonelt har definert sine nett som en del av Internettet, og følgelig med minimalt

med sikkerhetsbarrierer. Krav til akademisk frihet tilsier åpenhet og fravær av kontroll og logging av trafikk sier den tidligere IT-lederen.

Foruten disse momentene gjorde man en vurdering hvor man konkluderte med at enkel tilgang til bygningene og det kablede student-nettverket på dagtid kombinert med at bygningene lå tilbaketrukket og ble patruljert av vaktselskap på kvelden totalt sett kunne forsvare at man valgte en åpen løsning, gitt at denne bare ga tilgang til studentnettverket, hvor det i henhold til kontrakt med brukerne ikke skal oppbevares kritiske data.

IT-leder opplyser om at de kommer til å bytte løsning i nær fremtid, tentativt innenfor et halvt år. I søkendet etter en ny løsning har man lagt følgende til grunn; ønske om bedre sporbarhet, enkel og sentralisert administrasjon, gode muligheter for roaming mellom AP-er og studiesteder.

For å imøtekomme disse kravene har man valgt eduroam, en løsning som muliggjør nettvandring mellom mange utdanningsinstitusjoner i Europa. Løsningen baserer seg på et hierarki av RADIUS-servere, og det tilbys 802.1X autentisering med EAP-TLS, eller tunnelering av MS-CHAPv2 over EAP-TTLS eller PEAPv0. Konfidensialitet og integritet vil være beskyttet av TKIP eller CCMP. Innenfor disse rammene er det opp til den enkelte utdanningsinstitusjonen å gjøre de konkrete valgene av autentiserings- og sikkerhetsprotokoller.

6.3. Forespørsel til leverandører

På bakgrunn av at så mange av virksomhetene hadde støttet seg på leverandøranbefalinger, fant vi det nødvendig å kontakte 3 seriøse leverandører for å høre deres anbefalinger. Samtlige leverandører kunne opplyse om at de nå anbefalte løsninger basert på RSN og 802.11i, og da 802.1X autentisering gjennom PEAPv0-MSCHAPv2 for sikkerhet og kompatibilitet. Samtlige anbefalte sine kunder å benytte TKIP for konfidensialitet og integritet, da dette var ”sikkert nok” og det som fungerte flest steder, altså kompatibilitet med eksisterende utstyr uten behov for tilleggsprogramvare.

På forespørsel om hvorfor de anbefalte nettopp disse metodene for autentisering, integritet og konfidensialitet var svaret at det var sikkert nok, og at det var dette kundene ønsket.

På forespørsel om de kunne anbefale mer robuste løsninger, anbefalte èn av leverandørene EAP-TLS, med klientsertifkater på lokal harddisk, men opplyste om at de kun hadde gjort èn installasjon av løsningen i et forprosjekt for en kunde. EAP-TLS ble ikke valgt for autentisering grunnet kompatibilitetsproblemer og tidspress. På forespørsel om å benytte CCMP for konfidensialitet og integritet så anbefalte samtlige leverandører dette for optimal trådløs sikkerhet, men opplyste om nødvendigheten av å installere ekstra programvare på klienter. Ingen av deres kunder hadde så langt ønsket å ta denne ekstra jobben.

Ingen leverandører hadde erfaring med to-faktor autentisering under EAP-TLS eller PEAPv1-GTC.

7. Konklusjon empiri

Gjennom intervjuer med nøkkelpersonell i et utvalg norske virksomheter har det vist seg at man ikke benytter seg av det vi rangerer som de mest robuste standard-løsningene som er tilgjengelig for å sikre et WLAN.

En av virksomhetene har ikke tatt i bruk noen sikkerhetstiltak på sitt WLAN, mens en annen bruker pre-RSN metode, nemlig WEP og delvis MAC-adresse filter.

3 av virksomhetene benyttet RSN-metoder, men med det vi rangerer som den minst robuste av de Wi-Fi sertifisert autentiseringsmetodene i virksomhetsmodus. En av disse har, av kompatibilitetshensyn, i tillegg tatt i bruk WPA-PSK. Ingen krever bruk den mest robuste protokollen for konfidensialitet og integritet; CCMP. Av kompatibilitetsårsaker benytter man seg av TKIP, som er rangert etter CCMP.

Virksomhetene har ingen formening om hvorvidt de har valgt den sikreste løsningen. Dette kan forstås ut i fra at kun èn av virksomhetene hadde sikkerhet som en av de primære driverne for valg sikkerhetsløsning. Denne hadde også en oppfatning av at løsningen måtte oppgraderes for å være i samsvar med virksomhetens sikkerhetskrav.

Samtlige hadde støttet seg til leverandøranbefalinger, mens leverandørene på sin side paradoksalt nok opplyste om at de leverte løsninger basert på krav fra kunden.

Basert på en forventning om at virksomheter krever to-faktor autentisering fra eksterne nett, typisk en hjemmekontorløsning, hadde vi en antakelse om at dette ikke var tatt i bruk på WLAN-løsningen.

Det viste seg at samtlige hadde tilbud om fjernaksess, to av disse basert på en OTP-løsning. Høgskolen som har et helt åpent trådløst nettverk krever sertifikater for brukere som skal aksessere nettverket utenfor høgskolens lokaler og radiosignaler. Distributøren som benytter WEP-nøkkel og MAC-adressefilter på WLAN krever brukernavn og passord for fjerntilgang. VGS, som av kompatibilitetshensyn har måttet ha en WPA-PSK løsning i parallell med sin 802.1X-løsning, krever individuelt brukernavn og passord for fjerntilgang. Virksomhetene stiller altså strengere krav til autentisering fra andre eksterne nett enn fra det trådløse. I samsvar med våre antakelser kan disse da ikke sies å behandle det trådløse nettet som eksternt.

I de aktuelle virksomhetene har altså våre antakelser blitt bekreftet i alle så nært som ett tilfelle, nemlig forventningen vi hadde til at de selv trodde at de hadde valgt den sikreste løsningen. Dette hadde ingen av virksomhetene noen illusjoner om, så nær som èn hadde de ikke gjort denne vurderingen i det hele tatt.

8. Fremtidig arbeid

Videre følger to forslag til mulig fremtidig arbeid.

Forslag1) Som tidligere kommentert så viste Mørketallsundersøkelsen 2006 at 299 av totalt 749 norske virksomhetene benytter WLAN. En student ved HiG som har hatt tilgang til datagrunnlaget for Mørketallsundersøkelsen har på forespørsel fra undertegnede kjørt en korrelasjon mellom valg av autentiseringsløsninger og de virksomhetene som har trådløst nettverk. Dataene viser at av 299 virksomheter som tilbyr WLAN så benytter 19,7 prosent seg av smartkortløsninger, og 76,6 prosent seg av engangspassord. Tallene høres intuitivt høye ut, og er derfor dobbeltsjekket mot datagrunnlaget, men viste seg å stemme med dette[47]. Konklusjonen er altså at 96,3 av alle virksomhetene i undersøkelsen faktisk har infrastruktur til å ta i bruk to-faktor autentisering på trådløst nettverk. Med datagrunnlaget vil det altså være mulig å gå direkte på disse og se på hvor mange som faktisk gjør dette.

Opplysningene som vi innhentet fra tre leverandører var entydige, ingen av disse hadde implementert to-faktor autentiseringsløsning i WLAN produksjonsmiljø. Det ville vært ekstremt interessant å finne ut i hvilken grad virksomhetene i [NSR] har tatt i bruk, eller om de i det hele tatt har vurdert eller kjenner til muligheten av å benytte sine to-faktorløsninger også i WLAN.

Med utgangspunkt i vår intervjuguide og tilgang til datagrunnlaget fra mørketallsundersøkelsen vil det altså være mulig å gjøre en kvantitativ undersøkelse i kjølvannet av disse rapportene. Det vil åpenbart være oppsiktsvekkende dersom man kan predikere statistisk signifikans i tilknytning til valg og årsak til valg av sikkerhetsløsningene. Problemstillinger knapt har vært undersøkt på dette detaljnivået, og som vi bare i liten skala har berørt empirisk i vår rapport.

Forslag2)EAP-TLS ser ut til å være en svært robust metode for autentisering. Når ikke flere har valgt denne metoden vises det i litteraturen til at det er et tungt arbeid å få en PKI-infrastruktur på plass i virksomhetene, og at det ikke står i forhold til det man får igjen. Norge har i lengre tid arbeidet med å få på plass en *nasjonal* PKI-infrastruktur. Visjonen er at alle borgere skal få utstedt kvalifiserte elektroniske sertfikater etter lovens forstand, hvorvidt disse distribueres på et medium som gjør to-faktor autentisering mulig vites ikke, men dersom visjonen blir en realitet vil det antakelig være teknisk mulig å tilrettelegge for EAP-TLS autentisering også for virksomheters trådløse nettverk ved hjelp av denne infrastrukturen

Et fremtidig arbeid vil kunne være å analysere samhandlingsmulighet og potensielle synergieffekter mellom virksomheters trådløse-/trådbaserte nettverk og nasjonal PKI infrastruktur, og om det legges opp til at dette vil være tekniske mulig og sikkerhetsmessig forsvarlig at slik samhandling kan finne sted.

[47] Det høye tallet kan skyldes feil i selve datagrunnlaget, noe som ser ut til å ha forekommet i andre deler av [NSR], jf arbeidet til [AND].

9. Forkortelser

AAD	**additional authentication data**
AES	**advanced encryption standard**
AKMP	**Authentication and Key Management Protocol**
Anonce	**Authenticator nonce**
AP	**access point**
ARP	**Address Resolution Protocol**
AS	**Authentication Server**
BSS	**basic service set**
BSSID	**basic service set identification**
CBC	**cipher-block chaining**
CBC-MAC	**cipher-block chaining message authentication code**
CCM	**CTR with CBC-MAC**
CCMP	**CTR with CBC-MAC Protocol**
CTR	**counter mode**
EAP	**Extensible Authentication Protocol (IETF RFC 3748-2004 [RFC3748])**
EAPOL	**Extensible Authentication Protocol over LANs (IEEE Std 802.1X-2004)**
ESS	**extended service set**
GNonce	**group nonce**
GMK	**group master key**
GTK	**group temporal key**
GTKSA	**group temporal key security association**
IBSS	**independent basic service set**
ICMP	**Internet Control Message Protocol**
ICV	**integrity check value**
IrDA	**infrared data association**
MAC	**medium access control**
MPDU	**MAC protocol data unit**
MSDU	**MAC service data unit**
MSK	**master session key**
Nonce	**Number used once**
PDU	**protocol data unit**
PMK	**pairwise master key**
PTK	**Pairwise transient key**
PN	**packet number**
Pnonce	**peer nonce**
PRN	**pseudo-random number**
PRNG	**pseudo-random number generator**
PSK	**preshared key**
PTK	**pairwise transient key**
RADIUS	**remote authentication dial-in user service (IETF RFC 2865-2000 [B23])**
RSN	**robust security network**
RSNA	**robust security network association**
SA	**source address**
Snonce	**Supplicant nonce**

SPA	**Supplicant address**
SSID	**service set identifier**
STA	**station**
TA	**transmitter address or transmitting station address**
TKIP	**Temporal Key Integrity Protocol**
TSC	**TKIP sequence counter**
WEP	**wired equivalent privacy**

10. Definisjoner

additional authentication data Data som ikke er kryptert men ikke er kryptografisk beskyttet
advanced encryption standard En svært robust krypteringsalgoritme
Authentication and Key Management Protocol Et sett av en eller flere algoritmer some er designet for å tilby autentisering og nøkkelhåndtering (key management), enten individuelt eller i kombinasjon med høyere lags autentisering og nøkkelhåndterings algoritmer utenfor 802.11i standarden
Authentikator nonce Nonce brukt av autentikator. Se Nonce (Number used Once)
access point Enheten som tilbyr radiosignaler for trådløs tilgang. Oftest også autentikator.
Address Resolution Protocol Standard metode for å finne en nodes maskinvareadresse (MAC-adresse) basert på nodens IP-adresse
Authentication Server Enheten som tilbyr autentiseringstjenesten for en autentikator som kan gi eller avslå tilgang. I 802.11-nettverk er AS oftest en RADIUS-server
basic service set Et WLAN med ett AP og èn Service Set Identifier (SSID). Se dette
basic service set identification Ekvivalent med SSID. Se dette.
cipher suite Et sett av en eller flere algoritmer, designet for å tilby dataopprinnelse-integritet, konfidensialitet, integritet og/eller replay beskyttelse
CTR with CBC-MAC (Counter mode with Cipher-block chaining Message authentication code (CCM)) Et symmetrisk blokkchiffer som tilbyr konfidensialitet gjennom counter mode (CTR) og dataopprinnelse-integritet ved hjelp av Cipher-block chaining Message authentication code (CMC-MAC)
counter mode **Se over**
Extensible Authentication Protocol – EAP Se IETF RFC 3748-2004 [RFC3748]
Extensible Authentication Protocol over LANs Se IEEE Standard 802.1X-2004 [802.1X]
extended service set Et sett av en eller flere sammenkoblede BSS-er som fremkommer som et enkelt BSS (felles SSID) for link-laget (LLC) på ethvert STA assosisert med et av disse BSS-er.
framentering Segmentering av en MSDU i en sekvens av mindre MPDU-er før overføring finner sted. Den motsatte prosessen, å sette sammen MPDU-er til en MSDU kalles defragmentering
group Alle enheter som kommuniserer på et WLAN. F.eks AP og STA
group master key en nøkkel som brukes for å avlede group temporal key (GTK)

group temporal key En random verdi tilordnet fra broadcast/multicast kilden, som brukes for å beskytte broadcast/multicast MPDU fra kilden. GTK kan avledes fra GMK.
group temporal key security association Resultatet av en vellykket GTK utveksling enten via group key handshake eller et 4-way handshake.
IEEE 802.1X autentisering EAP autentiseringsdata som blir transportert av 802.1X protokollen
independent basic service set Et WLAN mellom ulike STA uten bruk av AP-er
Internet Control Message Protocol Beskrevet i RFC 792 og brukes hovedsakelig for testing av basis kommunikasjon mellom hoster i et TCP/IP-nettverk. Mest kjente bruk av ICMP er "ping" og "traceroute"(nix)/"tracert" (win)
integrity check value En verdi som verifiserer at en datapakke ikke er endret under transport.
infrared data association Kobling mellom to maskiner som støtter infrarød overføring
MAC protocol data unit Overføringsenheten som brukes på det fysiske laget mellom to noder på et WLAN
MAC service data unit Sammensettingen av MPDU-er. Se fragmentering.
master session key Nøkkelmateriale som avledes mellom EAP noden (STA) og AS.
Number used Once (Nonce) En verdi som i kryptografi assosieres med en gitt kryptografisk nøkkel, og som ikke må gjenbrukes med denne, heller ikke under noen reinitialisering gjennom systemets levetid
pairwise master key Den øverste nøkkelen i 802.11i nøkkelhierarkiet – se appendix F. PMK kan avledes fra en EAP-generert nøkkel eller fra en forhåndsdelt nøkkel (preshared key – PSK, jf. WPA-PSK)
pairwise transient key En verdi som ved hjelp av en pseudo-random funksjon (PRF) avledes fra PMK, autentikator adresse, supplikant adresse, autentikator nonce og supplikant nonce og splittes inntil 5 nye nøkler: temporal encryption key, to message integrity (MIC) nøkler, EAPOL-Key encryption key (KEK) og EAPOL-Key confirmation key (KCK). Disse 5 er utenfor rammene og detaljnivået i denne rapporten.
pseudo-random number generator En algoritme for generere en sekvens av tall som har "tilnærmet samme egenskaper" som et tilfeldig tall (random number). Helt random er det allikevel ikke.
preshared key En statisk nøkkel som distribueres til alle enhetene i systemet. For at nøkkelen ikke skal miste sin verdi i et kryptosystem må den overleveres via en sikker kanal og holdes hemmelig. Preshared key brukes fortrinnsvis om WPA-PSK, men en WEP-nøkkel er også i sin natur en preshared key.
remote authentication dial-in user service (IETF RFC 2865-2000 [B23]) en AAA (autentiserings, autoriserings- og accounting) protocol. I 802.11i virksomhetsnettverk er RADIUS-server analogt med AS, som er noden som avgjør om tilgang skal gis eller ikke.
robust security network

Et nettverk som kun tillater robust security network associations – RSNA. Se dette.
Robust security network association En forbindelse mellom to trådløse nettverksnoder som har blitt etablert gjennom et 4-way handshake. I praksis noder som benytter WPA eller WPA2.
Supplicant address MAC adressen til en 802.1X supplikant.
Station Formelt i hht 802.11i: Enhver enhet med et trådløst nettverkskort som interfacer mot det trådløse nettverket. I denne rapporten brukes STA som betegnelse på trådløse enhter som ikke er aksesspunkter. Typisk en bærbar PC.
Temporal encryption key Den delen av PTK eller GTK som brukes direkte eller indirekte for å kryptere data under overføring (MPDU-er)
Temporal key Kombinasjonen av temporal encryption key og temporal message integrity code (MIC) key
temporal message integrity code (MIC) key Den delen av transient key (TK) som sørger for integritet for MPDU-er og MSDU-er.
Temporal Key Integrity Protocol Sikkerhetsprotokoll for konfidensialitet og integritet i 802.11i som fikser alle kjente sårbarheter i WEP. WPA bygger på et TKIP-draft.
TKIP sequence counter Beskytter TKIP mot replay angrep ved å droppe pakker som ankommer i feil rekkefølge

11. Referanser

Alle refererte URL-er sist besøkt medio oktober 2007.

[802.11-1999] Institute of Electrical and Electronics Engineers Inc IEEE Std 802.11, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications 1999 Edition (R2003), IEEE 2003

[802.11i] Institute of Electrical and Electronics Engineers Inc. IEEE Std. 802.11i-2004, Amendment to Standard for Telecommunicatios and Informatio Exchange Between Systems – LAN/MAN Specific Requirements – Part 11: "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Security Enhancements, IEEE, 2004

[802.15] Institute of Electrical and Electronics Engineers Inc. IEEE Std 802.15.1 Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs)

[802.16] Institute of Electrical and Electronics Engineers Inc IEEE Std 802.16: A Technical Overview of the WirelessMAN Air Interface for Broadband Wireless Access, IEEE 2002

[802.1X] Institute of Electrical and Electronics Engineers Inc. IEEE Std 802.1X™-2004, IEEE Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control

[AND] Line S. Andersson, *Datakriminalitet i Norge*. Masteroppgave Høgskolen i Gjøvik, 2007

[AGG] Dr. A. K. Aggarwal, Aniss M. Zakaria, *A Survey on IEEE 802.11i Security Standard*, University of Windsor, 2004

[BIS] Matt Bishop *Computer Security Art and Science*, Pearson Education, 2003

[BIT] A. Bittau, M. Handley, J. Lackey, *The'Final' Nail in WEPs Coffin*
Proceedings of the 2006 IEEE Symposium on Security and Privacy (S&P'06) - Volume 00 Sider: 386 – 400, 2006

[BUS] Mark Jewell, *More accounts involved in TJX breach*, BusinessWeek Online, 24 oktober 2007

[BRI] Danny Briere, Pat Hurley *Wireless Network Hacks & Mods for Dummies*, John Wiley & Sons, 2005

[BRO]Edwin Lyle Brown, *802.1X Port-Based Authentication*, Auerbach Publications, 2007

[CAC] Johnny Cache, Vincent Liu *Hacking Exposed Wireless: Wireless Security Secrets & Solutions* McGraw-Hill/Osborne, 2007

[CHO] Suranjan Choudhury, Kartik Bhatnagar, Wasim Haque, NIIT *Public Key Infrastructure Implementation and Design*, John Wiley & Sons, 2002

[CIS03] Cisco Security Notice: *Dictionary Attack on Cisco LEAP Vulnerability*, Public Release 2003 August 03, Document ID: 44281 Cisco Systems, 2003
Tilgjengelig på: http://www.cisco.com/warp/public/707/cisco-sn-20030802-leap.shtml

[COM1] *WLAN Security Executive* Article in Computerworld Ref. [VAC]

[CSI05] 2005 *CSI/FBI Computer Crime and Security Survey,* Computer Security Institute Publications, 2005

[CSI06] 2006 *CSI/FBI Computer Crime and Security Survey,* Computer Security Institute Publications, 2006

[CSI07] 2007 *CSI/FBI Computer Crime and Security Survey,* Computer Security Institute Publications, 2007

[DAN] Ram Dantu et al, *EAP methods for wireless networks*. Computer Standards & Interfaces, tilgjengelig elektronisk på ScienceDirect 27 September 2006.

[DOM] Arbaugh sitert på CNN EleKtronisk tilgjengelig på http://archives.cnn.com/2002/TECH/industry/02/18/wifi.security.idg/index.html

[EDN] Edney Jon, Arbaugh William *A. Real 802.11 Security Wi-Fi Protected Access and 802.11i* © 2004 Pearson Education

[FAL] Magnus Falk, *Fast and Secure Roaming in WLAN*, Masteroppgave Linkøpings Universitet 2004

[FMS] Scott Fluhrer, Itsik Mantin, Adi Shamir, *Weaknesses in the Key Scheduling Algorithm of RC4* (udatert, publisert i august 2001), 23pp.
Presentert p Eighth Annual Workshop on Selected Areas in Cryptography, August 2001.

[FUN] Paul Funk, Simon Blake-Wilson, *EAP Tunneled TLS Authentication Protocol draft-ietf-pppext-eap-ttls-04*,PPPEXT Working Group, Internet-Draft, Internet Engineering Task Forse (IETF), 2004

[FRA] C. Frankfort-Nachmias, D. Nachmias, D, *Research methods in the social sciences* (4. utgave), St. Martin's Press, 1992

[GAS] Matthew Gast *802.11 Wireless Networks: The Definitive Guide*, O'Reilly & Associates, 2002

[GAS02] Matthew Gast. *A Technical Comparison of TTLS and PEAP*. http://www.oreillynet.com/pub/a/wireless/2002/10/17/peap.html, 2002.

[GOL] *Computer Security,* Dieter Gollman, John Wiley & Sons, 2006

[HAN] Wei Han, Dong Zheng, Ke-fei Chen *Some Remarks on the TKIP Key Mixing Function of IEEE 802.11i* Shanghai Jiaotong University, Dept. of Computer Sci. & Eng. China National Laboratory for Modern Communications, som henviser til [MOE]

[HAR] Thomas Hardjono and Lakshminath R. Dondeti *Security in Wireless LANs and MANs,* Artech House, 2005

[HE] Changhua He, Johns C Mitchell, *Security Analysis and Improvements for IEEE 802.11i,* Electrical Engineering and Computer Science Departments
Stanford University, The 12th Annual Network and Distributed System Security Symposium (NDSS'05), pages 90-110. Feb. 2005

[HAN] Lei Han, *A threat analysis of The Extensible Authentication Protocol*, Honors Project Report, Carleton University 2006

[HELL] Helleset Hallvard *Wi-Fi Security How to break and exploit*, Master Thesis University of Bergen 2006

[HEL] Hellman M. *A cryptanalytic time-memory trade-off*.,IEEE Transactions on Information Theory, 26:401-406, 1980

[HOF] D. Hoffman, *Blackjacking: Security Threats to BlackBerry Devices, PDAs, and Cell Phones in the Enterprise,* John Wiley & Sons, 2007

[HOL] Hole, Kjell Jørgen, *Open Wireless University Networks Risk Analysis and Mitigation* versjon 2, NoWires Research Group, Department of Informatics, University of Bergen, 2007, http://www.kjhole.com/WebSec/PDF/OpenNets.pdf

[HUR1] Chris Hurley et al How *to Cheat at Securing a Wireless Network,* Syngress Publishing, 2006

[HUR2] Chris Hurley et al WarDriving: Drive, Detect, Defend: A Guide to Wireless Security, Syngress Publishing, 2004

[HUS] M. Hussain, M. Akbar, M. Muft, S. Kanhere, *Piggy Back Challenge Based Security Mechanism for IEEE 802.11i Wireless LAN CCMP Protocol*. School of computer Science and Engineering. Universitiy of New South Wales&Information Security Department National University of Sciences and Technology., Pakistan, 2006

[HOS] Nettstedet til epitest.fi, langURL tilgjengelig fra http://tinyurl.com/29ltvd

[JOS] S. Josefsson et al *Protected EAP Protocol (PEAP) draft-josefsson-pppext-eap-tls-eap-05*, PPPEXT Working Group, Internet-Draft, Internet Engineering Task Forse (IETF), 2002

[KB823731] *How to remove cached user credentials that are used for PEAP authentication in Windows XP* Knowledge base ArticleID: 823731 http://support.microsoft.com/default.aspx?scid=kb;en-us;823731

[KB893357] The Wi-Fi Protected Access 2 (WPA2)/Wireless Provisioning Services Information Element (WPS IE) update for Windows XP with Service Pack 2 Article ID: 893357, Microsoft Corporation 2005, http://support.microsoft.com/kb/893357/en-us

[KB917021] *Description of the Wireless Client Update for Windows XP with Service Pack 2*, Article ID: 893357, Microsoft Corporation 2007, http://support.microsoft.com/kb/917021/en-us

[KHA] Djamel Khadraoui, Francine Herrmann (redaktorer) *Advances in Enterprise Information Technology Security,* IGI Publishing, 2007

[KLE] Andreas Klein *Attacks on the RC4 streamcipher*, Designs, Codes and Cryptography, 2007.

[KNA] Svein J. Knapskog, *Informasjonssikkerhet i internett,* Tapir Akademisk Forlag 2005

[KVA] Steinar Kvale, *Det kvalitative forskningsintervju*, Ad Notam Gyldendal, 1997

[LEI] J. Leira, P. Bjørbak, *802.1X for trådløse nettverk,* Uninett 2004

[LON] Johnny Long et al. Wireless Penetration Testing Using Auditor Penetration Tester's Open Source Toolkit, Syngress Publishing, 2006

[MAL] Kirsti Malterud *Kvalitative metoder i medisinsk forskning : en innføring* 2. utg Universitetsforlaget, 2003

[MCG] David McGrew Counter Mode Security: Analysis and Recommendations", Cisco Systems, 2002

[MIS] Mishra A Petroni N, Arbaugh W, Fraser T. *Security issues in IEEE802.11 wireless local area networks:a survey* University of Maryland Wireless Communications and Mobile Computing 2004; 4:821–833

[MOE] (WPA weakness TKIP WPA moen et al.pdf) *Weaknesses in the temporal key hash of wpa*, Moen, Vebjørn, Raddum, Håvard, Hole, Kjell J. Department of informatics university of Bergen

[NOK] Nettverk og kommunikasjon, *Forstå Trådløs sikkerhet*, Frode Sørensen, IDG Press Nummer 3 2006.

[NIST800-97] NIST Special Publication 800-97 Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i

[NIST800-48] NIST Special Publication 800-48 *Wireless Network Security, 802.11*

[NORSIS] – Nettstedet til Norsk senter for informasjonssikring www.norsis.no

[NSM] – Nasjonal Sikkerhetsmyndighet Sårbarheter og og trusler mot informasjonssystemer. Temahefte 1/2006. 2006

[NTA] NTA Monitor (2002). *The 2002 NTA Monitor Password Survey*. Tilgjengelig pa http://www.nta-monitor.com/fact-sheets/pwd-main.htm , Besøkt 17.12.04

[NSR] Mørketallsundersøkelsen 2006. Næringslivets Sikkerhetsråd, 2007

[NUUG] Mæland J, *Foredrag medlemsmøte 2005-01-13*: Norsk Unix System Brukers Forening (NUUG), 2005

[NWF] Weinberg N, *Security Survey*, Network World, 05/08/00 http://www.nwfusion.com/research/2000/0508secsurvey.html

[OU1] George Ou – *The six dumbest ways to secure a Wireless LAN. Wireless LAN security hall of Shame*. http://blogs.zdnet.com/Ou/index.php?p=43 18 Mars 2005

[OU2] George Ou *Wireless LAN Security Guide* http://www.lanarchitect.net/Articles/Wireless/SecurityRating/

[PFL] C Pfleeger C & S Pfleeger *Security in Computing*, 3dje utgave, Prentice Hall, 2003

[PKCS#15] ~ ISO/IEC 7816-15. http://www.rsa.com/rsalabs/node.asp?id=2141

[PRA] Anand R. Prasad and Neeli R. Prasad, *802.11 WLANs and IP Networking: Security, QoS, and Mobility* Artech House,2005

[REG] *Taxis Hailed a Black Hole as Confidential Data gets Taken for a Ride* http://www.theregister.co.uk/2005/01/25/taxi_survey/ og http://www.checkpoint.com/press/pointsec/2005/01-24b.html

[RIT]John Rittinghouse and James Ransome, *Wireless Operational Security,* Digital Press, 2004

[RFC1661] W. Simpson (red.) RFC 1661 Standards - The Point-to-Point Protocol (PPP), IETF 1994

[RFC2284] L. Blunk, J.Vollbrecht. RFC 2284 Standards - PPP Extensible Authentication Protocol (EAP). IETF, 1998.

[RFC2401] S. Kent, R.Atkinson, RFC 2401 Standards - Security Architecture for the Internet Protocol, IETF 1999

[RFC2607] B.Aboba, J. Vollbrecht RFC 2607 Informational - Proxy Chaining and Policy Implementation in Roaming, IETF 1999

[RFC2865] C. Rigney et al, RFC2138 Standards - Remote Authentication Dial In User Service (RADIUS), IETF, 2000

[RFC3162] B. Aboba, G. Zorn, D. Mitton *RFC 3162 Standards - RADIUS and IPv6*, IETF, 2001

[RFC3579] B. Aboba, P.Calhoun, RFC3579 Informational - RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP), An update to RFC 2869 IETF, 2003

[RFC3749] S. Hollenbeck RFC 3749 Standards- Transport Layer Security Protocol Compression Methods, IETF, 2005

[RFC4017] D. Stanley, J. Walker, B Aboba, RFC 4017 Informational - Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs, IETF, 2005

[RFC3748] B. Aboba et al RFC 3748 Standards - Extensible Authentication Protocol (EAP), IETF 2004

[RFC2749] G. Zorn Microsoft PPP CHAP Extensions, Version 2, IETF, 2000

[ROO] A class of weak keys in the RC4 stream cipher. September 1995

[RSA] *The Power Behind RSA SecurID Two-factor User Authentication: RSA ACE/Server, Solution White Paper*, RSA Security Inc 2001 http://www.opsec.com/solutions/partners/downloads/rsa_securid_whitepaper.pdf

[RSA1] *Securing WLANs with two-Factor Authentication* : RSA Solution White Paper, RSA Security Inc 2006 http://www.rsaconference.com/uploadedFiles/RSA365/Security_Topics/Wireless/White_Papers/RSA/RSA_Securing_WLANs.pdf

[SAN] K Sanka, A. Balinsky, D. Miller, S. Sundaralingam *EAP Authentication Protocols for WLANS*, Cisco Press, 2005 http://www.ciscopress.com/articles/article.asp?p=369223&rl=1

[SCHI] Robert Schifreen Defeating the Hacker: A Non-Technical Guide to Computer Security, John Wiley & Sons, 2006

[SCH1] Bruce Schneier, Crypto-Gram Newsletter March 15, 2000

[SCH2] Bruce Schneier, *Applied Cryptography* Second edition, John Wiley & Sons, 1996

[SIS] *Sikkerhetsmekanismer i trådløse nett*, Senter for informasjonssikring 25.4.2005

[SKO] Ed Skoudlis, Sans Institute *Intervju i Network World*, 03/21/05

[STA] William Stallings, *Network Security Essentials* Second Edition, Prentice Hall 2002

[STMLD17] *Stortingsmelding nr 17 (2006-2007) Eit informasjonssamfunn for alle*, Det Kongelege Fornyings- og Administrasjonsdepartement, 2006

[SYM1] Et sikkert IT-miljø, *Hva små og mellomstore bedrifter må vite for å kunne skape et sikkert IT-miljø*. Kundskaparna Strategi/Symantec Corporation 2007 ISBN 978-91-976811-1-7

[SYM2] *Spørreundersøkelse på oppdrag av Symantec*: Online QuestBack-undersøkelse 11-25 april 2007 med e-postinvitasjon til utvalg på 2500 IT-ansvarlige i små og mellomstore bedrifter, 0 - 250 ansatte, 300 svarte på undersøkelsen Tilgjengelig på http://www.symantec.com/no/no/about/news/release/article.jsp?prid=20070531_01

[UNI] Uninett ABC *Sikkerhet i trådløse nett*. Temahefte. Tilgjengelig på http://www.uninettabc.no

[TEW] Erik Tews, Ralf-Philipp Weinmann, Andrei Pyshkin *Breaking 104 bit WEP in less than 60 seconds*, Technische Universitat Darmstadt, 2007 http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/

[VAC] John Vacca, *Guide to Wireless Network Security*, Springer Verlag, 2006

[VIE] John Viega, GaryMcGraw, Building Secure Software: How to Avoid Security Problems the Right Way, Addison-Wesley Professional 2001

[VLA] Andrew Vladimirov et al, Wi-Foo: *The Secrets of Wireless Hacking*, Addison-Wesley Professional, 2004

[WAL] Jesse Walker, *Unsafe at any key size; An analysis of the WEP encapsulation*/ IEEE 802.11-00/362, Intel Corporation, 2000

[WALL] Joseph Pereira, *Breaking the Code. How Credit-Card Data Went Out Wireless Door*, The Wall Street Journal Online, 4 mai 2007

[WIFI] Wi-Fi Alliance *Annual Report 2006* Wi-Fi Alliance 2006

[WON] Stanley Wong; *The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards*, SANS Institute, 2004

[WRI03] Joshua Wright Abusing 802.11: Abusing 802.11:Weaknesses in LEAP Challenge/Response – Innlegg på Defcon 3 august 2003
http://asleap.sourceforge.net/asleap-defcon.pdf

[X.800] ITU - International Telecommunication Union, *Recommendation X.800*

Data communication networks: Open systems Interconnections (OSI); Security Structure and applications, Security Architecture for open systems interconnection for CCIT applications, ITU 1991

[ZOW] Dino A. Dai Zovi, Shane A. Macaulay, *Attacking Automatic Wireless Network Selection*, Proceedings of the 6th IEEE SMC Information Assurance Workshop, "The West Point Workshop", IEEE, 17 juni 2005

Appendiks A Analyseverktøy

Et lite utvalg av verktøy for analyse av sikkerheten på WLAN:

• Verktøy	• Muligheter	• Kilde	• Kommentar
AirSnort	War Driving, Pakkesniffing	Open-source: http://airsnort. shmoo.com	Finner WEP-nøkler (Windows/Linux)
WEPCrack	Pakkesniffer	Open-source: http://wepcrack.sourceforge.net	Finner WEP-nøkler (PERL basert)
Wireshark	Pakkesniffer	Open-source: http://wireshark.com	Basert på Libpcap, et pakkesniffer bibliotek (tekst og GUI basert)
Tcpdump	Pakkesniffer	Open-source: http://tcpdump.org	Basert på Libpcap, et pakkesniffer bibliotek (kun tekstbasert)
Sniffer Wireless	Pakkesniffer & Analyse	Kommersielt produkt fra Network Associates: www.nai.com	Dekryptering av WEPtrafikk og deteksjon av uatorisert AP (Windows/PDA)
Net Stumbler	WarDriving; Kartlegging	Open-source: http://netstumbler.com	Finne SSID - interaksjon, mot GPS (Windows/PDA)
Kismet	WarDriving; Kartlegging Pakkesniffer	Open-source: http://kismetwireless.net	Populært og omfattende Wardriving verktøy.
Wellenreiter	WarDriving; Kartlegging Pakkesniffer	Open-source: http://www.wellenreiter.net	Perl og C++ based for Linux
AiroPeek & OmniPeek	WarDriving; Kartlegging Pakkesniffer	Kommersielt produkt fra WildPackets http://www.wildpackets.com	Egnet for feilsøking, overvåking og sikring av WLAN
Aircrack-ng	Pakkesniffer, analyse, injection og spoofing	Suite bestående av 4 komponenter: airodump, aireplay, aircrack, airdecap http://aircrack-ng.org/	Verktøykasse for WPA og WEP crack. Windows Linux:

• Verktøy	• Muligheter	• Kilde	• Kommentar
			Generering av støtte for pakke injection for raskere recovery tid på nøkler
CoWPAtty	Analyse av WPA	http://www.remote-exploit.org/	Ordliste og bruteforce angrep på PSK. Joshua Wright
Asleap-imp	Analyse av LEAP	http://www.remote-exploit.org/	Ordliste og bruteforce angrep på MS-Chap Joshua Wright
Leap	Analyse av LEAP	http://www.packetstormsecurity.org	Ordliste- og bruteforce angrep på MS-Chap Skrevet av DaBubble, Bishop, Evol.
KARMA	Cloaking angrep	http://theta44.org	Basert på [ZOV]

Alle nettsteder sist besøkt 29.10.07

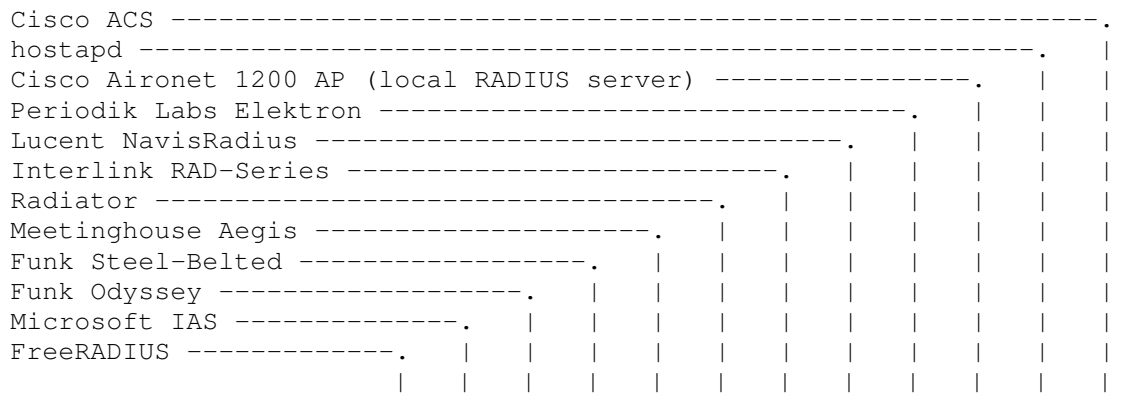
Appendiks B EAP metoder og kompatibilitet

Hentet fra hostap.epitest.fi. For full URL se [HOS]

Matrisen er utarbeidet for kontrollere støtte for et driverprosjkt under linux, men mer interessant markerer den støtten RADIUS-server har for en del kommersielle og gratis

Metoder supportert av Wi-Fi alliance er merket med **fete typer**. Metoder som er relevante for drøftingen i denne oppgaven er merket **<u>med fete typer og understreking</u>**.

```
Test matrise
+) tested successfully
F) failed
-) server did not support
?) not tested
```



EAP-MD5	+	–	–	+	+	+	+	+	–	–	+	+
EAP-GTC	+	–	–	?	+	+	+	+	–	–	+	–
EAP-OTP	–	–	–	–	–	+	–	–	–	–	–	–
EAP-MSCHAPv2	+	–	–	+	+	+	+	+	–	–	+	–
EAP-TLS	**+**	**+**	**+**	**+**	**+**	**+**	**+**	**+**	**–**	**–**	**+**	**+**
EAP-PEAPv0/MSCHAPv2	**+**	**+**	**+**	**+**	**+**	**+**	**+**	**+**	**+**	**–**	**+**	**+**
EAP-PEAPv0/GTC	+	–	+	–	+	+	+	+	–	–	+	+
EAP-PEAPv0/OTP	–	–	–	–	–	+	–	–	–	–	–	–
EAP-PEAPv0/MD5	+	–	–	+	+	+	+	+	–	–	+	–
EAP-PEAPv0/TLS	–	+	–	+	+	+	F	+	–	–	–	–
EAP-PEAPv1/MSCHAPv2	–	–	+	+	+	+	+	+	+	–	+	+
EAP-PEAPv1/GTC	–	–	+	+	+	+	+	+	+	–	+	+
EAP-PEAPv1/OTP	–	–	–	–	–	+	–	–	–	–	–	–
EAP-PEAPv1/MD5	–	–	–	+	+	+	+	+	–	–	+	–
EAP-PEAPv1/TLS	–	–	–	+	+	+	F	+	–	–	–	–
EAP-TTLS/CHAP	+	–	+	+	+	+	+	+	+	–	+	–
EAP-TTLS/MSCHAP	+	–	+	+	+	+	+	+	+	–	+	–
EAP-TTLS/MSCHAPv2	+	–	+	+	+	+	+	+	+	–	+	–
EAP-TTLS/PAP	+	–	+	+	+	+	+	+	+	–	+	–
EAP-TTLS/EAP-MD5	+	–	+	+	+	+	+	+	+	–	+	–
EAP-TTLS/EAP-GTC	+	–	+	?	+	+	+	+	–	–	+	–
EAP-TTLS/EAP-OTP	–	–	–	–	–	+	–	–	–	–	–	–
EAP-TTLS/EAP-MSCHAPv2	+	–	+	+	+	+	+	+	+	–	+	–
EAP-TTLS/EAP-TLS	–	–	+	+	F	+	+	+	–	–	–	–
EAP-SIM	+3	–	–	?	–	+	–	?	–	–	+	–
EAP-AKA	–	–	–	–	–	+	–	–	–	–	+	–
EAP-PSK	+7	–	–	–	–	+	–	–	–	–	+	–
EAP-PAX	–	–	–	–	–	+	–	–	–	–	+	–
EAP-SAKE	–	–	–	–	–	–	–	–	–	–	+	–
EAP-GPSK	–	–	–	–	–	–	–	–	–	–	+	–
EAP-FAST/MSCHAPv2(prov)	–	–	–	+	–	–	–	–	–	+	–	+
EAP-FAST/GTC(auth)	–	–	–	+	–	–	–	–	–	+	–	+
EAP-FAST/MSCHAPv2(aprov	–	–	–	–	–	–	–	–	–	–	–	+
EAP-FAST/GTC(aprov)	–	–	–	–	–	–	–	–	–	–	–	+
EAP-FAST/TLS(aprov)	–	–	–	–	–	–	–	–	–	–	–	+
EAP-FAST/MSCHAPv2(auth)	–	–	–	–	–	–	–	–	–	–	–	+
EAP-FAST/TLS(auth)	–	–	–	–	–	–	–	–	–	–	–	+
LEAP	+	–	+	+	+	+	F	+	–	+	–	+

Appendix C Oversikt over angrep

Kartleggings og proof-of-concept av [HELL]

Attack	Service	Requirements	Approximate Time
RC4	Confidentiality, Authentication	300,000 WEP encrypted frames	20 minutes
WEP dictionary	Confidentiality, Authentication	Pass-phrase seeded key, 1 data frame	Norwegian word list in 5 sec.
Chosen plaintext	Confidentiality	WEP enabled. Allow 10 byte data size	50 minutes for full frame
Redirect	Confidentiality	WEP enabled	Insignificant
Double encryption	Confidentiality	Internet connection	At least a few hours
One way auth	Authentication	Shared-key authentication	Insignificant
Spoofing	Authentication	1 active and authenticated client	Insignificant
Rogue access point	Authentication	1 client	Insignificant
Packet injection	Access control	Known IV/key sequence	Insignificant
Profiling	Access control	Known IV/key sequence	Insignificant
MAC filter	Access control	MAC filter enabled	Insignificant
Captive Portal	Access control	MAC filter access control	Insignificant
WPA-PSK dictionary	Confidentiality, Authentication	Pass-phrase seeded key, handshake	Norwegian word list in 1 hour

Appendix D - Intervjuguide

Tilbyr virksomheten tilgang til trådløst nettverk WLAN
Hvis ja, hvor lenge har dere hatt det?

Har virksomhetene PKI-infrastruktur?
Ja/Nei/Fremtidig
Hvis Ja; hvordan håndteres tapte sertifikater (CRL)?
Hvis fremtidig: kommer WLAN til å benytte dette?

Har virksomheten RADIUS-server
Ja/Nei/Kan installeres uten ekstra kostnad

Benytter virksomheten 2-faktor autentisering?

Har virksomheten mulighet for fjerntilgang/hjemmekontor?
Hvilken metode benyttes?

Hva var primær driver for valg av WLAN-løsning?
Sikkerhet
Ytelse
Kompatibilitet
Lett å rulle ut/implementere
Kostnad
Stabilitet
I tråd med sikkerhetspolicy
Annet?

Hva var valget over basert på
Egen kunnskap – hvor har man så denne kunnskapen fra? Studier formelle/uformelle?
Leverandørs anbefaling
Annen kunnskap

Planer om å bytte miljø i nær fremtid?
Hvilke primære egenskaper ser dere evt etter i en fremtidig løsning

Hva slags klientmiljø?
MAC, Windows, Nix, PDA?

Hvilken tilgang gir WLAN?
Til gjestenett eller kun for internett-aksess
Er personopplysninger tilgjengelig fra WLAN (må dere forholde dere til POL)

Hva var primær driver for valg av krypterings-løsning?
Sikkerhet
Ytelse
Kompatibilitet

Lett å rulle ut/implementere
Kostnad
Stabilitet
I tråd med sikkerhetspolicy
Annet?

Hvordan sikrer dere nettet deres i dag mhp konfidensialitet og integritet:
Krypteringsmetode
CCMP
TKIP
CCMP/TKIP mix
WEP 40 bits? 104 bits?
RSN/TSN mix?
Ingen

Hva var primær driver for valg av autentiserings-løsning?
Sikkerhet
Ytelse
Kompatibilitet
Lett å rulle ut/implementere
Kostnad
Stabilitet
I tråd med sikkerhetspolicy
Annet?

Hvilke primære autentiseringsmetoder bruker dere i dag
EAP-TLS m/2 faktor – Smartkort. Tiltak i forhold til tyveri. CRL?
EAP-PEAPv1 GTC – Validering av serverside sertifikat?
EAP-TTLS-GTC – Validering av serverside sertifikat? WIDS?
EAP-TLS – Tiltak i forhold til stjålne enheter?
EAP-PEAPv0 MS-CHAPv2 – Tiltak i forhold til bortkomne enheter? Slette registry
EAP-TTLS MS-CHAPv2 – Tiltak i forhold til bortkomne enheter?
LEAP – Sterke passord?
EAP-MD5
Annet?
WPA-PSK – Sterke passord, tiltak i forhold til bortkomne enheter
WEP 40, 104 annet Sterke passord, tiltak i forhold til bortkomne enheter
WEP+lavnivåmetode – hvilken lavnivå metode?
MAC adresse filtrering

***Hvis enterprise EAP-metode:**
Plassering av RADIUS/AS-server?
Sikkerhetsmekanismer mellom AP og RADIUS?
- kompleksitet på shared secret
- predefinert sett AP-er som kan kommunisere med AS?
- IPSec

***Hvis PSK:**

- hva er endringsintervall på PSK-bytte?
- kompleksitet på shared secret

Har dere implementert andre (lavnivå) sikkerhetsmekanismer
Skjult SSID
DHCP slått av
MAC adresse filtrering
Fake SSID
Antenneplassering – Hvordan er antennen plassert
Sticky page
Captive Portals – hvor står portalen infrastrukturmessig

Andre sikkerhetmekanismer av betydning for WLAN sikkerhet?

Appendix E Svar på intervju

Den Videregående Skolen
Navn: Person A
Navn: Person B
Stilling: Førstekonsulent

Tilbyr virksomheten tilgang til trådløst nettverk WLAN
Hvis ja, hvor lenge har dere hatt det?
4 år – klasserom bibliotek

Antall brukere totalt og på WLAN
1900 elever
400 ansatte
Alle har i prinsippet tilgang til WLAN

140 basestasjoner på 36 000 kvadratmeter. Fabrikant 3com

Har virksomhetene PKI-infrastruktur?
Nei

Har virksomheten RADIUS-server
Ja – Freeradius – Linux-basert

Benytter virksomheten 2-faktor autentisering?
Ja, men bare for tilgang til sensitive opplysninger om vanskeligstilte elever. Tjenesten tilbys av fylkeskommunen og ligger utenfor lokalt driftsansvar. Gjenbruk av token virker lite sannsynlig.

10 av cirka 400 ansatte har denne tilgangen

Har virksomheten mulighet for fjerntilgang/hjemmekontor?
Det gis tilgang over en Novell-proprietær løsning kalt Netdrive for å gi tilgang til elevnettverket. Denne baserer seg på brukernavn og passord og krever klient programvare fra Novell. Ressursen gir tilgang til elevens hjemmeområde og elevenes fellesområde.

Hva var primær driver for valg av WLAN-løsning?
Primær driver for valg av WLAN løsning var først og fremst kravet fra ledelsen om å tilby en fleksibel løsning for å ivareta skolens gode rennomè.

Hva var valget over basert på?
Føringer fra Uninett og Fylkeskommunen

Planer om å bytte miljø i nær fremtid?
Nei

Hva slags klientmiljø?

Apple MACintosh, Linux, Windows

Hvilken tilgang gir WLAN?
3 WLAN –
"Gjestenett" – Web portal (låst mot elevnett – http)

"VGS-Radius" – primærnett for elevene mot edirectory VLAN tildeles på bakgrunn av brukerident.

"WPA-nettverk – PSK". Stasjonære elevpc-er og klassesett bærbart.

Er personopplysninger tilgjengelig fra WLAN (må dere forholde dere til POL)
Nei

Hva var primær driver for valg av krypterings-løsning?

Captive Portal
Fleksibilitet – gjester får tilgang via engangspassord som deles ut av IT-sekretær

RADIUS/WPA
Krav fra fylket at man skulle ha TKIP.

For sistnevnte mente fylkeskommunen at det var "sikkert nok" med TKIP.

WEB Portalen gir kun internett-tilgang og virksomheten stiller ingen spesielle krav til kryptering i denne sonen.

Hvordan sikrer dere nettet deres i dag mhp konfidensialitet og integritet:
Krypteringsmetode
WPA, RADIUS: TKIP
Captive Portal: Ingen

Hva var primær driver for valg av autentiserings-løsning?
RADIUS-Fylkets sikkerhetspolicy – føring

WPA: Praktisk løsning for å kunne kjøre login-script. Praktiske årsaker –nødvendig å kjøre loginscript noe som man i dag kun klarer å løse ved å kjøre WPA-PSK. Nettet er nødvendig da man har klassesett med PC-er som kan trilles rundt og settes inn ved behov.

Captive Portal: fleksibilitet

Hvilke primære autentiseringsmetoder bruker dere i dag
RADIUS
EAP-PEAPv0 MS-CHAPv2

Tiltak i forhold til bortkomne enheter? Nei
Offisielt sertifikat? Nei, selvgenerert

Godkjenning av serversertifikat: Nei
Flushing av cachet passord i registeret? Nei

WPA-nettet
WPA-PSK ikke sterke passord (5 tegn). Ingen faste endringsintervall på nøkler (så langt)

WEB-portal
Passord som gir tilgang i et døgn

Ingen lav-nivå sikkerhetstiltak

***Hvis enterprise EAP-metode:**
Plassering av RADIUS/AS-server?
På vmware på server-elevnettet (VLAN151) – åpent nett for alle VLAN

*Sikkerhetsmekanismer mellom AP og RADIUS?
- kompleksitet på shared secret – Liten
- predefinert sett AP-er som kan kommunisere med AS? Ja
- IPSec eller annen kryptering - Nei

*Hvis PSK:
- hva er endringsintervall på PSK-bytte? Intet
- kompleksitet på shared secret-Lav (5 tegn)

Har dere implementert andre (lavnivå) sikkerhetsmekanismer
Nei

Captive Portals – hvor står portalen infrastrukturmessig? VX-en er WLAN kontroller og står på en trunk-port som plasserer disse forespørslene i et eget segment i infrastrukturen. Segmentet gir kun internett-tilgang.

Annet; litt om nettet:
2 RADIUS-servere for redundans.
SVS har rogue aksesspunkt deteksjon og system for å jamme ned disse.

Petroleumsvirksomheten
Navn: Person A
Navn: Person B
Stilling: IT Professional

Tilbyr virksomheten tilgang til trådløst nettverk WLAN
Hvis ja, hvor lenge har dere hatt det?
Drøyt 1 år

Kun WLAN i fjortende/øverste etasje på hovedkontoret
Et gjeste WLAN og et VirksomhetsWLAN

244 bærbare og 150 stasjonære på dette kontoret

Virksomheten har totalt 4000 pc-er hvorav 1200 bærbare som potensielt kan være brukere på WLAN

Har virksomhetene PKI-infrastruktur?
Nei
Ikke planer om dette heller i fremtiden

Har virksomheten RADIUS-server
Ja – MS IAS

Benytter virksomheten 2-faktor autentisering?
Ja for remote access. RSA SecurID

Har virksomheten mulighet for fjerntilgang/hjemmekontor?
4 stk. Cisco VPN – Concentrator 3000 m/ krav RSA SecurID

Hva var primær driver for valg av WLAN-løsning?
God erfaring med leverandør, Cisco
Fordi det var Cisco – som alt annet nettverksutstyr
Kompatibilitet
Krav om internett for gjester

Hva var valget over basert på
Kompatibilitet
Leverandør sin kunnskap

Planer om å bytte miljø i nær fremtid?
Nei og heller ingen planer om utvidelser
Man sliter med kompatibilitet på eksisterende bærbart utstyr. Det vil innebære en betydelig økonomisk investering å bytte ut alt dette utstyret. Dagens nettverkskort på

majoriteten av utstyr blir jammet av de trådløse signalene i valgt løsning (Compaq-ene går i "blue-screen")

Hva slags klientmiljø?
Windows XP

Hvilken tilgang gir WLAN?
Gjestenett/internett-aksess
Virksomhetsdata/Kundedata

Hva var primær driver for valg av krypterings-løsning?
Kompatibilitet

Anbefaling fra leverandør

Hvordan sikrer dere nettet deres i dag mhp konfidensialitet og integritet:
Krypteringsmetode
CCMP/TKIP mix
Captive portal i gjestenett

Hva var primær driver for valg av autentiserings-løsning?
Gjestenett: Pris
Virksomhetsnettverk: Anbefaling fra leverandør
Gjenbruk av Microsoft Supplikant og Microsoft IAS RADIUS server. Ønsket seg Cisco, men for dyrt.

Hvilke primære autentiseringsmetoder bruker dere i dag?
EAP-PEAPv0 MS-CHAPv2

***Hvis enterprise EAP-metode:**
Plassering av RADIUS/AS-server? LAN
Sikkerhetsmekanismer mellom AP og RADIUS?
- kompleksitet på shared secret – Ingen krav til passordkompleksitet
- predefinert sett AP-er som kan kommunisere med AS? - Ja
- IPSec - Nei

***Hvis PSK:**
N/A

Har dere implementert andre (lavnivå) sikkerhetsmekanismer
Antenneplassering –Antennene er plassert 14 etasje.
Rogue Access Point detection (deteksjon av falske AP-er) - JA

Andre sikkerhetmekanismer av betydning for WLAN sikkerhet
Kryptering av disker
BIOS-passord
Passordbytte hver 90 dag.

Salgsvirksomheten
Navn: Person A
Stilling: IT driftssjef

Tilbyr virksomheten tilgang til trådløst nettverk WLAN
2 stk Cisco WLAN Controller i Cluster sentralt i Norge. Virksomheten er i 12 land. Det tilbys trådløst i 4 land.

93 AP. Ca: 25000kvm

Like mange SSIDer som kontorer.
Kommunikasjonen mellom WLAN kontroller og "dumme AP-er" på utekontorer fraktes over MPLS

IT Minst fra 2005.
Antall brukere totalt og på WLAN:

Har virksomhetene PKI-infrastruktur?
Nei -men virksomheten har planer om dette fremtidig
Dette vil benyttes i fremtidig løsning i kombinasjon med med biometri/fingeravtrykk

Har virksomheten RADIUS-server
Microsoft IAS

Benytter virksomheten 2-faktor autentisering?
Nei ikke pr i dag. Om 2 uker vil man ta i bruk en løsning for tilsending av kode til mobiltelefon - RSA Løsning

Har virksomheten mulighet for fjerntilgang/hjemmekontor?
Løsningen baserer seg på brukernavn og passord inn mot en SSL VPN concentrator. Denne gir tilgang til Citrix Terminal sesjon. Det er mulighet for å laste ned Active X control for å aksessere virksomhetens ressurser på filnivå.

Hva var primær driver for valg av WLAN-løsning?
Standardisering
Sikkerhet
Forutsigbarhet
Cisco

Hva var valget over basert på?
Teknologileder Cisco
Nærhet til kompetanse på løsningene
Høy teknisk kvalitet på produktene
Kompatibilitet med eksisterende utstyr.

Planer om å bytte miljø i nær fremtid?
Ja – man kommer til å bytte autentiseringsmetode til 2 faktor

Hva slags klientmiljø?
Windows, Linux (utviklere) Ubuntu, Nokia

Hvilken tilgang gir WLAN?
WLAN gir kun tilgang til SSL VPN løsning over port 3389 og autentiserer videre derfra.

WLAN droppes ned i ulike VLAN basert på SSID
Gjestenett gir tilgang til Captive portal med strupet pipe kun til internett.

Virksomhetene må forholde seg til PCI-standarden fra en større kredittkortleverandør. Denne tillater ikke at kundedata er tilgjengelige fra WLAN.

Administrativt ansatte får uten videre tilgang til mail og kontorstøtteapplikasjoner. For ytterligere tilgang kreves terminalsesjon

Hva var primær driver for valg av krypterings-løsning?
Et minimum i PCI standard. Kompliance.
Kompatibilitet (Håndholdte enheter (PDA-er) fra Symbol –fungerer ikke med CCMP)

Hvordan sikrer dere nettet deres i dag mhp konfidensialitet og integritet:
Krypteringsmetode
TKIP
Ingen mulighet for å velge lavere eller høyere

Hva var primær driver for valg av autentiserings-løsning?
Sikkerhet
Ytelse
Kompatibilitet
Anbefalinger fra leverandør
I samsvar med PCI standard

Hvilke primære autentiseringsmetoder bruker dere i dag
EAP-PEAP-MS-CHAPv2

*Hvis enterprise EAP-metode:
Plassering av RADIUS/AS-server?

Sikkerhetsmekanismer mellom AP og RADIUS?
kompleksitet på shared secret: Ja
predefinert sett AP-er som kan kommunisere med AS? Ja
IPSec Ja.

Andre relevante sikkerhetstiltak i forhold til WLAN?
Captive Portals – hvor står portalen infrastrukturmessig? Egen sone.
Rogue Access Point detection (deteksjon av falske AP-er). Detekterer dem. Kan gjøre ARP-poison.
IDS

Tiltak ved tapt enhet: Sperrer bruker.
Passordsikkerhet: Krever mer enn 14 tegn, under ledernivå: 8 tegn
Kryptering av disk for mellomleder og opp.
Krever passordbytte hver 60 dag
Krever passordkompleksitet, dvs kombinasjon av små/store bokstaver, tall og spesialtegn

Høgskolen
Navn: Person A, Person B
Stilling: Nåværende IT Leder og avdelingsdirektør; tidligere IT-leder.

Virksomheten: Høgskole i Norge med 3 studiesteder
2700 studenter, 250 ansatte, Totalt over 3000 potensielle brukere

Tilbyr virksomheten tilgang til trådløst nettverk WLAN
Hvis ja, hvor lenge har dere hatt det?
Studiested 1: 2001 – 12000 kvm, 90 % WLAN dekning 13 AP-er
Studiested 2: 2003 – ca 10 000 kvm
Studiested 3 :2007 – 9000 kvm, 100 % WLAN dekning

Har virksomhetene PKI-infrastruktur?
Ja, klientsertifikater for hjemmekontorløsning

Har virksomheten RADIUS-server
Ja. Freeradius, men benyttes ikke lengre. Tidligere brukt for mac adresselister på det ene studiestedet.

Benytter virksomheten 2-faktor autentisering?
Nei

Har virksomheten mulighet for fjerntilgang/hjemmekontor?
Ja. Lag 3 OpenVPN – løsning. Sertifkater på klienter.

Hva var primær driver for valg av WLAN-løsning?
Standardisering innenfor Høgskolesektor – Cisco.
Sikkerhet gikk på at man etablerte på studentsiden.
Ikke WEP fordi – kultur i systemet – så ikke noen sikkerhetsmessig oppside i WEP.
Administrativt slitsomt.
Bygget var åpent allikevel.
Ytelse througput.
Sikkerhetspolicy

Hva var valget over basert på
Cisco ble anbefalt av Uninett.
Omforent oppfatning av at Cisco var bra
Bra innkjøpspris
Egen kunnskap
Vanlig i høgskolesektoren
Åpenhet og fravær av kontroll på trafikk – akademisk frihet.
Kurs/fagpress/kontakter i høgskolemiljøet
Geografisk utilgjengelig.

Planer om å bytte miljø i nær fremtid?
Eduroam. Hierarki av RADIUS servere. Roaming mellom læresteder i Europa.

Ønsker å bytte fordi: sporbarhet. Tilgjengelighet, roaming, enklere administrasjon (i forhold til Mac-adresser)

Hva slags klientmiljø?
Windows, MAC, enkelte Linux

Hvilken tilgang gir WLAN?
Studentnett. Tilgang til administrativt nett over VPN, men flere sikkerhetsbarrierer til POL.

Hva var primær driver for valg av krypterings-løsning?
Ikke aktuelt pga åpent system

Hvordan sikrer dere nettet deres i dag mhp konfidensialitet og integritet:
Krypteringsmetode
Ingen

Hva var primær driver for valg av autentiserings-løsning?
Ikke aktuelt pga åpent system

Hvilke primære autentiseringsmetoder bruker dere i dag
Ingen

Har dere implementert andre (lavnivå) sikkerhetsmekanismer
Skjult SSID på ett studiested
DHCP lease varer i 12 timer

Distributøren
Navn: Person A
Stilling: Konstituert IT-sjef

Lokalt driftsansvar på alt annet enn firewall
Norge: 125-130 ansatte
Totalt: Over 2 tusen ansatte
Omsetning 2 milliarder i Norge 32 milliarder.
10 kontorer, 9 Land.

Tilbyr virksomheten tilgang til trådløst nettverk WLAN
Cirka et år.

Har virksomhetene PKI-infrastruktur?
Nei

Har virksomheten RADIUS-server
Kan installeres uten ekstra kostnad. Microsoft IAS.

Benytter virksomheten 2-faktor autentisering?
Nei

Har virksomheten mulighet for fjerntilgang/hjemmekontor?
Ja. Hvilken metode benyttes? Lag3 VPN klient fra Nortel.
I tillegg Microsoft Lavere lags VPN-klient - PPTP
Terminalservere i DMZ – tilgjengelig uten VPN-klient.

Hva var primær driver for valg av WLAN-løsning?
Behov for tilgang. Startet i Warehouse, basert på MAC-adresser.
2 nett
1 Warehouse: Kompatibilitet. Roaming. ”få det til å funke”. Brand: HP
1 Husnett: Roaming. Brand: HP

Hva var valget over basert på
Leverandør anbefaling på kravspec. Fikke ikke noe annet MAC-adresse filter til å fungere på W2K-Prof maskiner i lageret.

Planer om å bytte miljø i nær fremtid?
Hvilke primære egenskaper ser dere evt etter i en fremtidig løsning
Ja. Roaming, dekning, gjestenett. Pris. På forespørsel: Sikkerhet. Sikkerhet vil bli prioritert mer og mer i tiden fremover.

Hva slags klientmiljø?
Windows XP, Windows 2000 – i trucker.

Hvilken tilgang gir WLAN?
2 WLAN - Kontor og Warehouse/Lagernett

Er personopplysninger tilgjengelig fra WLAN (må dere forholde dere til POL). Nei, men kundedata i CRM og logistikksystem.

Hva var primær driver for valg av krypterings-løsning?
Lager: Manglende kryptering; Roaming
Husnett: Sikkerhet – sikrere enn 64. En standardløsning.

Hvordan sikrer dere nettet deres i dag mhp konfidensialitet og integritet:
Krypteringsmetode
Husnett: WEP, 104 bit.
Warehouse: Ingen

Hva var primær driver for valg av autentiserings-løsning?
Sikkerhet i husnettet. At det var sikkert nok. Sikrere enn 40 bit.
Kompatibilitet – MAC filter i Warehouse på W2K PC-er.
Lett å rulle ut/implementere

Hvilke primære autentiseringsmetoder bruker dere i dag
WEP
MAC adresse filtrering

Sperrer bruker. Sperrer VPN-klient.

*Hvis enterprise EAP-metode:
N/A

***Hvis PSK:**
- Ingen endringsintervall på WEP-nøkkel
- Krav til kompleksitet på WEP-nøkkel: skulle være lett å huske. Internkonkurranse.

Har dere implementert andre (lavnivå) sikkerhetsmekanismer
Nei

Appendix F - Nøkkelhierarki

Fra [PRA]

- (Str,F,L): from Str starting from left to right, extract bits F through F+L−1.
- PRF-n: pseudorandom function (PRF) producing n bits of output. PRF is a function that hashes various inputs to derive a pseudorandom value (the key).

The PMK is used to create pairwise transient keys (PTKs). Transient keys are used for confidentiality algorithms and their maximum lifetime is PMK lifetime. PTKs are created for each association. The PTK consists of EAPOL-key confirmation key (KCK), the EAPOL-key encryption key (KEK), and temporal keys (TKs) for TKIP and CCMP. In the following these keys and their use are explained (see Figure 4.18, where the AA is the authenticator address and the SPA is the supplicant address).

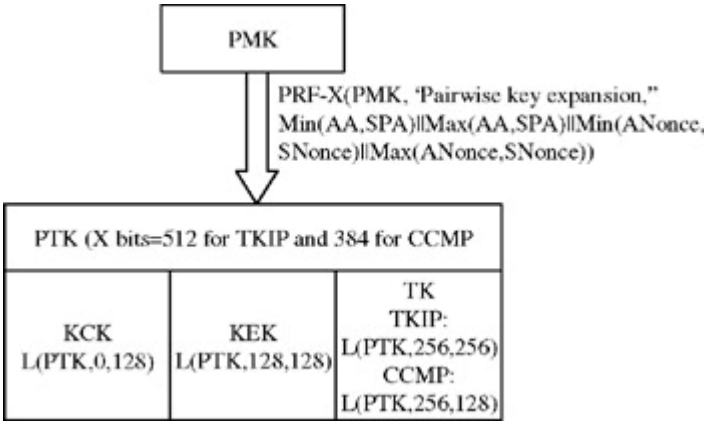


Figure 4.18: Pairwise key hierarchy

- KCK: It is 128 bits and is used by IEEE 802.1x in a 4-way for data origin authenticity. One can also call this key the integrity key.
- KEK: This is also 128 bits long and is used by handshake to provide confidentiality.
- TKs for TKIP: TKIP makes use of RC4, which only had the possibility for encryption. Thus TKs in TKIP consist of the integrity and encryption keys of 128 bits each. Bits 0–127 of TKs are input to the TKIP phase 1 and 2 mixing functions (see Section 4.5.8), (i.e., for encryption). Bits 128–191 of TK are used as the Michael key [i.e., integrity key for MAC service data units (MSDUs) from the authenticator (AP) to the supplicant (STA)] while bits 192–255 are used as the Michael key for MSDUs from the STA to the AP. Note that a MSDU is a packet of data between the software and the MAC in contrast to the MAC Protocol Data Units (MPDUs) which are the MAC layer packets. Thus a MPDU can be a portion of the MSDU if the MSDU is bigger than MPDU.
- TKs for CCMP: In case of CCMP both encryption and integrity are incorporated in a single calculation. Thus there is one key of length 128 bits.
- KeyID 0 is used when sending a pairwise key.