

## 802.11i: Endelig reell WLAN sikkerhet?

*Vi har gått gradene – fra WEP til WPA og tilbake, og deretter videre til sentraliserte sikkerhets- og aksessmekanismer for våre trådløse nettverk. Hver gang en ny standard, mekanisme eller løsning dukker opp, rettes oppmerksomheten mot svakhetene knyttet til eksisterende mekanismer, og hvor viktig det er å komme til neste nivå. Kun unntaksvis nevnes utfordringene som følger med på kjøpet – at en nykommer kan være inkompatibel med eksisterende utstyr eller for komplisert til at den lar seg sette ut i livet.*

### Oppsummering

802.11i er ingen revolusjon, og får på kort sikt praktisk betydning først og fremst for store miljøer og miljøer som skal benytte trådløs IP-telefoni.

Følgende punkter oppsummerer nykommerens viktigste egenskaper og konsekvenser:

- Mens 802.11i er standarden, er WPA2 spesifikasjonen nye produkter vil bli testet etter. WPA2 omfatter alle obligatoriske deler av 802.11i.
- WPA2 er et supersett av WPA og kompatibelt med denne. WPA-klienter vil fungere i et WPA2-miljø.
- Mange produkter som i dag støtter WPA kan oppgraderes til WPA2 via programvare. Siden de nye krypteringsalternativene i WPA2 krever betydelig mer prosesseringskapasitet, er mulighetene for en slik oppgradering imidlertid ingen selvfølge. Likeledes vil ressurssvake klienter (eldre PCer, PDAer etc.) vanskelig kunne benytte de nye krypteringsalternativene.
- Virksomheter med mer enn noen få brukere bør benytte RADIUS-autentisering via 802.1X- og EAP-standardene. Det er påvist sikkerhetsmessige svakheter i RADIUS-standardene de siste må-

nedene som nødvendiggjør spesiell oppmerksomhet i forbindelse med konfigureringen av et slikt system.

- Det er identifisert problemstillinger i tilknytning til *roaming* og autentisering som ikke er tilfredsstillende ivare tatt av 802.11i. IEEE har nedsatt en ny gruppe med betegnelsen 802.11k som studerer disse (telefoni-relaterte) problemstillingene.
- Full utnyttelse av mekanismene i 802.11i forutsetter at vi har kontroll over både klienter og aksesspunkter. Dette er ikke tilfelle i forbindelse med offentlige IP-soner, hvilket betyr at den nye standarden ikke har noen praktisk betydning i den forbindelse.
- WPA2-sertifiserte produkter kommer på markedet i denne måneden.

Uansett hvilke behov vi har i dag, er 802.11i en viktig milepæl for sikring av WLAN. På et eller annet tidspunkt i overskuelig fremtid vil de problemstillingene standarden adresserer også banke på nettopp vår dør. Da er det betryggende å vite at mekanismene ikke bare finnes, men at de er standardiserte og har hatt tid til å modnes i praktisk bruk.

### Smertefull fortid

Sikkerhetsproblemer har forfulgt trådløse lokalnett siden de kom på markedet i 1999, og har i perioder skremt deler av markedet fra å ta teknologien i bruk. Temaet har også vært oppe til diskusjon en rekke ganger her i Mellvik-Rapporten, hvor vi har lagt vekt på betydningen av en realistisk holdning til utfordringene.<sup>2</sup> I diskusjoner om krypteringsalgoritmer, nøkkelutvekslinger og autentiseringsmekanismer har hovedpoengene lett for å bli borte: De største sikkerhets-utfordringene – her som i andre sammenhenger – har med brukere og driftspersonell å gjøre, ikke med teknologi. Skandalene og redselshistoriene knyttet til

<sup>2</sup> Se for eksempel "Mer trådløshet, mer hodepine" på side 27.

**WEP** – *Wired Equivalent Privacy*

**WPA** – *Wi-Fi Protected Access*

**AES** – *Advanced Encryption Standard*

**EAP** – *Extended Authentication Protocol*

### Trådløs alfabetsuppe

Om bransjen i sin alminnelighet er beryktet for sin omgang med forkortelser, er situasjonen ikke så ille at det ikke kan bli verre. Og verre er det definitivt i WLAN-segmentet – ikke minst i leverandørenes egen litteratur. Hakk i hæl følger uavhengige eksperter og analytikere – med Gartner Groups 'First Take' om 802.11i (1.7.04) som foreløpig topp: 18 forkortelser i et avsnitt på 13 linjer, som i tillegg til å være praktisk talt uleselig også inneholder faktiske feil. Dette lover ikke godt...

### Bruk WPA!

Vår konstatering av at WEP fortsatt er dominant og at det ikke alltid er mulig å bruke WPA selv om den finnes, er ikke det samme som en anbefaling av WEP. WEP er bedre enn ingen ting, må kombineres med andre tiltak, og brukes kun der ingen bedre alternativer finnes.

Anbefalingen er med andre ord: **Bruk WPA eller WPA2!**

### Utvidet standard for nye behov

WLAN har i de fleste tilfeller vært forårsaket av feilkonfigurering, avslåtte sikkerhets-mekanismer og banale passord. Å diskutere sikkerhet utover den opprinnelige WEP-krypteringen før disse elementene er under kontroll, har lite for seg.

### Mange svakheter, flere misforståelser

Mens WEP-krypteringen har kjente svakheter og kan knekkes, er den ikke verdiløs. De fleste krypteringsmekanismer lar seg knekke over tid, og det relevante spørsmålet er hvor ressurskrevende en slik knekking er – hvor høy er barrieren? Sikkerhetsdebatter har lett for å glemme at perfekt, 100% sikkerhet ikke finnes, og at det alltid er graden av sikring vi diskuterer. WEP hever terskelen fra null til et nivå som kan sammenlignes med å låse døren. Med WPA-standarden (se Mellvik-Rapporten nr. 100, 109 og 113) fikk vi sikkerhetslås på døra og bedre kontroll med hvem som har nøkler. Bedre og mer omfattende sikkerhet betyr imidlertid også høyere kompetansemessig terskel og støtter utfordringen i forbindelse med samspill mellom utstyrstyper. Høyere kompleksitet er i seg selv en trussel – som i tilfellet WPA er håndterbar, men definitivt mer krevende for brukere uten teknisk kompetanse enn WEP.

Derfor burde det ikke komme som en bombe på noen at WEP-128 – typisk kombinert med VPN – fortsatt er den dominante sikringsmekanismen for trådløse nettverk. En annen årsak til at WEP lever i beste velgående er at kombinasjonen *roaming* og WPA er problematisk for de fleste utstyrstyper, spesielt i den lave enden av skalaen.

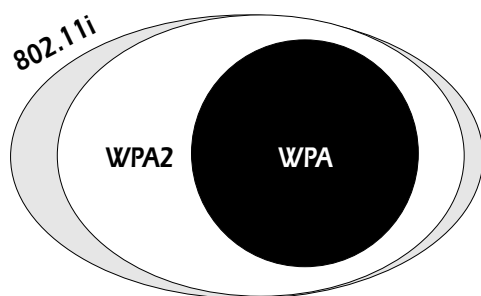
### Mye vil ha mer ...

Siden WPA tar vare på alle kjente svakheter i WEP og enda mer – er ikke behovene dermed dekket? Dersom vi tar utgangspunkt i dagens marked, der WEP av praktiske hensyn fortsatt er den dominerende mekanisme for transportsikring, og WPA dekker tilleggsbehovene, er svaret ja. Den siste tilveksten på sikkerhetsfronten – 802.11i – har ikke som primær målsetting å heve sikkerhetsnivået ytterligere, men å løse praktiske problemer i kjølvannet av nye anvendelser. Samtidig er det ingen grunn til å stikke under en stol at nykommeren også tilgjengeliggjør mekanismer for ytterligere heving av transport-sikkerheten – med utgangspunkt i den relativt ferske krypteringsstandarden AES – *Advanced Encryption Standard*.

Den korte innholdsfortegnelsen for 802.11i, som ble ratifisert i sommer, blir dermed:

- ✘ Tilgang til enda sikrere låser (sterkere kryptering).
- ✘ Sikre distribusjonsmekanismer for nøkler.
- ✘ Støtte for sikring av klient-til-klient (p2p) forbindelser i tillegg til klient-tjener forbindelser.
- ✘ Mekanismer for *caching* og effektiv overføring av nøkler og autentiserings-informasjon mellom aksesspunkter.

Spesielt siste punkt – kombinasjonen autentisering og *roaming* – for tjener oppmerksomhet når nytteverdien av den nye standarden skal diskuteres. Mekanismer for overføring av brukere i bevegelse fra ett



**Figur 1** Både WPA og WPA2 dekker deler av hele 802.11i-standarden. WPA2 omfatter hele standarden med unntak av valgfrie elementer – som er notriske kilder til inkompatibiliteter når en standard skal implementeres.

aksesspunkt til det neste har eksistert lenge, men har vært vanskelige eller umulige å kombinere med skikkelig sikkerhet. Vi har hatt valget mellom *roaming* eller sikkerhet, og har som regel valgt det første – gjerne supplert med separat sikring via VPN. En slik løsning skalerer dårlig og er notorisk problematisk på tvers av utstyrsleverandører. Dessuten stiller nye anvendelser – med VoIP i spissen – strenge krav til rask overføring (*handover*) av klienter i bevegelse. Disse kravene har nødvendiggjort introduksjonen av nye mekanismer for sikker og pålitelig caching av

autentiserings-informasjon og rask, transparent re-autentisering når klienten 'overtas' av et nytt aksesspunkt.

Som referansen til VoIP avslører, er tidsaspektet spesielt relevant. I tillegg til at autentiserings-prosessen tidligere verken var behørig sikret eller godt standardisert, var den også for tidkrevende. Takket være en særdeles aktiv deltagelse i standardiseringsarbeidet fra WLAN-industrien, har det lyktes å komme frem til løsninger som dekker de behovene vi ser i dag og i nær fremtid.<sup>3</sup> Tiden for re-autentisering er redusert med en størrelsesorden – fra typisk 0,5 - 0,8 sekunder til under 50 millisekunder.

### Fokus på autentisering

Autentiseringen foregår på samme måte som i WPA – via en kjent nøkkel (tilsvarer passord, *shared key* på fagspråket), eller via en bakenforliggende RADIUS-tjener – i henhold til den etterhvert velkjente 802.1x-standarden. Første alternativ fungerer bra kun for små miljøer med noen få brukere og skalerer dårlig.

RADIUS-autentisering<sup>4</sup> har vært i bruk i forbindelse med fjerninnlogging og oppringte forbindelser i over 10 år, og har bred støtte i alle tenkelige systemer. Siden svært mange miljøer allerede har en RADIUS-tjener i drift, er steget over til skikkelig WLAN-autentisering relativt beskjeden. I LAN- (og WLAN-) sammenheng utvides RADIUS-mekanismene med EAP-protokollen som sørger for at selve autentiserings-transaksjonen blir sikret. Kombinasjonen og samspillet er spesifisert i en egen standard (802.1x, som vi nevnte ovenfor), og er i løpet av de siste 2-3 årene blitt den foretrukne mekanismen for sikker nettverksautentisering. [Vi gjennomgår funksjonelle og praktiske detaljer i forbindelse med 802.1x-standarden i neste utgave, se baksiden for detaljer.]

3 Det er samtidig blitt avslørt problemstillinger som ikke lar seg løse innenfor dagens standard. IEEE har satt ned en ny arbeidsgruppe som studerer disse problemstillingene og eventuelt kommer opp med forslag til løsninger. Gruppen har fått betegnelsen 802.11k.

4 Se Mellvik-Rapporten nr. 56 for en gjennomgang av RADIUS. Utgaven er tilgjengelig i pdf-format via vår Web-tjeneste, se side 35.

**RADIUS** – Remote Authentication Dial-In User Service

**EAP** – Extensible Authentication Protocol

**SANS** – System Administration and Network Security

Arbeidet med 802.11i og den voksende utbredelsen av 802.1x i LAN-sammenheng, har avslørt enkelte svakheter i RADIUS som har vakt betydelig oppmerksomhet i fagpressen de siste månedene. Mens disse svakhetene er reelle nok, er de forårsaket av implementasjoner som avviker fra anbefalingene i IETF-standarden RFC2865. Sikkerhets-eksperter fra organisasjonen SANS Institute og leverandøren Aruba Wireless Networks arbeider i disse dager med et forslag til presisering og innstramming av RADIUS-standarden som på sikt vil eliminere disse problemene. I mellomtiden er det verdt å være oppmerksom på at de finnes, og ikke minst at en 'inntrenger' må ha fysisk tilgang til lokalnettet (mellom RADIUS-tjener og trådløse svitsjer eller basestasjoner) for å kunne utnytte dem.

## Konklusjon

Reell WLAN-sikkerhet ble tilgjengelig sammen med WPA-spesifikasjonen i 2003. 802.11i-standarden vil først og fremst ha betydning for organisasjoner med spesielt høye krav til transportsikkerhet og som katalysator for trådløs VoIP.

Som standarder flest inneholder 802.11i en rekke opsjoner og implementeringsvalg. At et produkt er i overensstemmelse med standarden gir derfor ingen garanti for at det kan spille sammen med andre produkter.

WPA2 og sertifiseringen som utføres av Wi-Fi-organisasjonen, tar vare på denne utfordringen. Derfor er det WPA2-merking vi skal forlange fra våre leverandører.

Dagens produktgenerasjon støtter WPA, som er kompatibel med WPA2, og vil være dominant i 2-3 år fremover. I løpet av perioden vil WPA2-implementasjonene bli modne og robuste, og klar til å levere pålitelig og effektiv WLAN-sikkerhet i de fleste sammenhenger. At tidsperspektivet er såpass langt, betyr imidlertid ikke at vi skal vente med å forlange WPA2 fra våre leverandører. Uten trykk fra markedet går fremskrittene med sneglefart. ■

### Fakta om WPA2 og 802.11i

- WPA2 (*Wi-Fi Protected Access version 2*) er utarbeidet av bransjesammenslutningen Wi-Fi ([www.wi-fi.org](http://www.wi-fi.org)), og er en spesifisering som skal legges til grunn ved testing av produkter. Godkjente produkter får rett til å bære en spesiell logo fra Wi-Fi. De første produktene passerte nåløyet 1. september. Flere titalls produkter ligger i kø for testing og godkjenning fremover høsten.
- Som tilfellet har vært for tidligere spesifikasjoner fra Wi-Fi (den forrige var WPA fra 2003, se Mellvik-Rapporten nr. 110), er hensikten å gi markedet trygghet for at produktene ikke bare overholder standarden, men også kan spille sammen. Enhver standard er for 'løs i kantene' til at overholdelse alltid er det samme som full kompatibilitet.
- WPA2 overlapper IEEE 802.11i-standarden, men utelater elementer som er valgfrie, og som dermed ikke har (eller har negativ) innflytelse på interoperabilitet på tvers av produkter.
- WPA2-produkter er bakoverkompatible med den forrige WPA-standarden, som var basert på en uferdig 802.11i-standard. Det betyr at klienter som kjøper WPA kan spille med en WPA2-aksess-infrastruktur.
- Den viktigste forskjellen mellom WPA og WPA2 er at sistnevnte støtter nye og 'sterkere' krypteringsmekanismer – med blant annet nøkkellengder opp til 256 bits og mekanismer for kontinuerlig forandring av aktive nøkler. AES, som krypteringen er basert på, ansees for å være praktisk talt uknekkelig i dag.
- Mange WPA-produkter på markedet kan oppgraderes til WPA2 ved å bytte *firmware*, som for de fleste er en enkel prosess. Utstyret må ha støtte for AES-kryptering i hardware for at en slik oppgradering skal være mulig.
- Som WPA har WPA2 to modi: Den 'personlige' er tilpasset konsument-markedet og benytter et forhåndsdefinert passord som krypteringsnøkkel. I 'profesjonell' modus benyttes 802.1x- og EAP-standardene for autentisering og automatisk distribusjon av krypteringsnøkler. Slik autentisering forutsetter at en brukerkatalog og en RADIUS-tjener som kan levere autentiserings-tjenesten er tilgjengelig.
- Mens WPA kom på banen på grunn av påviste svakheter i forgjengeren WEP, er så ikke tilfelle med WPA2.
- WPA2-sertifisering er for alle praktiske formål en bekreftelse av at produktet har implementert 802.11i-standarden på en måte som er kompatibel med andre implementasjoner.