

# God sikkerhet krever 802.1X

Artikkelen følger opp vår fokusering på 802.11i-standarden for trådløs sikkerhet i forrige utgave, Mellvik-Rapporten nr. 120.

*Sikring av infrastruktur betyr å slippe inn de som skal ha adgang og stoppe alle andre. Så enkelt er det å formulere målet – som de fleste av oss vet kan være svært så krevende å få til i praksis. Og – for god ordens skyld – vi snakker i denne sammenheng om aksess og autentisering, ikke om trafikk-kontroll.*

Mens de fleste sikkerhets- og nettverksansvarlige vi er i kontakt med, mener å ha god kontroll og oversikt over hvem som får tilgang til infrastrukturen, er det fortsatt forbausende få som har tatt i bruk 802.1X-standarden. Argumentet vi hører er gjerne at “situasjonen er under kontroll allerede, 802.1X er for komplisert”. Mens dette høres greit ut, er det for de fleste miljøer med fra et tosifret antall brukere og oppover, feil. Om etablerte løsninger basert på mer eller mindre proprietære mekanismer og standarder fungerer i dag, er sjansen for at de vil være tilfredsstillende i morgen, beskjeden. Problemstillinger som skalerbarhet, oversikt og fysisk aksess – og i noen tilfeller begrensninger i leverandørspesifikke, proprietære løsninger, blir til slutt for kompliserte og kostbare å leve med.

## Kontroll over fysisk tilgang

Som tilfellet er i mange sammenhenger, er enkelhet en hovedingrediens i løsningen. Årsaken til at de fleste eksisterende mekanismer og løsninger ikke skalerer, er at de er for kompliserte og krever for mye innsats for å holde ved like. Kontroll-mekanismene ligger ofte inne i nettverket i stedet for helt ytterst – i strid med såvel teori som praksis for effektiv sikring gjennom tusenvis av år.

Den enkle målsettingen for effektiv aksesskontroll skal være å sørge for at **kun autoriserte brukere får FYSISK tilgang til nettverket**. Om det er mulig? Javisst, men som vi skal se, må vi justere en smule på vår oppfatning av hva ‘fysisk tilgang’ betyr.

For tradisjonelle (kabelbaserte) lokalnett (LAN) har vi besørget fysisk sikring gjennom deaktivering av ubrukte porter på kantsvitsjene, og låsing av fysiske porter til spesifikke MAC-adresser. Første generasjons WLAN-aksesspunkter fulgte opp denne modellen ved å benytte aksesskontroll-lister (ACLs), som åpnet for spesifikke MAC-adresser og blokkerte alle andre. Disse mekanismene er enkle å forstå og å konfigurere, men vanskelige å følge opp i en dynamisk hverdag. Dessuten gir de fleste moderne nettverkskort brukeren mulighet til å forandre MAC-adressen, hvilket vesentlig reduserer sikringseffekten av slike aksesslister.

802.1X-standarden – *the LAN Port Access Control Framework* på fagspråket – tar tak i denne utfordringen, og kombinerer en rekke velkjente mekanismer og standarder til et rammeverk som fungerer like godt for trådløse som kabelbaserte nettverk.

**MAC-adresse** – lavnivå-adresse som er unik for selve grensesnittet (Medium Access Control)  
**ACL** – Access Control List

## Motivasjon

Mens forfalskede MAC-adresser er mulig i både kabelbaserte (LAN) og trådløse (WLAN) lokalnett, er risikoen vesentlig større i WLAN. En besøkende uten eskorte kan riktignok finne MAC-adressen på en maskin, legge den inn i sin egen, koble over nettverkskabelen, og på den måten komme 'på nett'. Øvelsen forutsetter imidlertid fysisk adgang til både lokaler og nettverk, hvilket i seg selv er – eller skal være – en betydelig barriere å forsere.

I WLAN-sammenheng er problemstillingen langt enklere. En potensiell inntrenger kan med lett tilgjengelig utstyr og verktøy avlytte nettverket på god avstand, notere gyldige MAC-adresser, omkonfigurere sin egen maskin, sende en frakoblingsmelding på vegne av maskinen som eier adressen, og deretter umiddelbart ikle seg dens rolle og koble seg opp. Ingen fysisk tilgang til lokaler eller nettverk er nødvendig. Inntrengeren kan befinne seg i gangen, i resepsjonen, på toalettet eller over gaten.

Om risikoforskjellen mellom LAN og WLAN er betydelig, er det likevel åpenbart at robuste mekanismer for aksesskontroll er nyttige og ønskelige for begge situasjoner. Dessuten har vi et tredje scenario som krever oppmerksomhet: Brukeraksess fra Internettet, der typiske sikringsmekanismer er filtrering på IP-adresser kombinert med en eller annen form for VPN på høyere nivå. Mens slike mekanismer er påkrevet, er de ikke på egen hånd tilstrekkelige til å gi den nødvendige aksesskontroll. For eksempel:

- ✓ Bruk av statiske IP-adresser, som er lettvinnt og var alminnelig før sikkerhet for alvor kom på agendaen, gir enda mindre beskyttelse enn filtrering på MAC-adresser. En inntrenger kan 'sniffe' seg frem til gyldige adresser, eller sågar gjette riktig etter å ha prøvd en stund.
- ✓ Dersom brukerinnloggingen foregår ukryptert over nettverket, kan en 'sniffer' lett snappe opp både brukernavn og passord. Er passordet 'hashet' (en triviell form for koding som lenge har vært brukt av Windows), vil tilgjengelige verktøy kunne avsløre dem i løpet av sekunder eller minutter.
- ✓ Inntrengere kan også gjøre skade uten å ha kommet seg gjennom brannmur og rutere ved å sette i gang såkalte DOS-angrep – mot selve brannmuren eller mot ressurser innenfor.

Ved å kanalisere oppkoblinger fra Internettet gjennom de samme mekanismene som 802.1X foreskriver for LAN og WLAN, og kombinere disse med sikringsmekanismer på høyere nivå, kan truslene reduseres eller elimineres fullstendig.

Sett fra et fugleperspektiv er problemstillingene sammenfallende: Om brukeren kommer inn via LAN, Internett eller WLAN, er tilgang til lokalnettet selve målet, forutsetningen for å få gjort den jobben som presumptivt skal gjøres. Derfor er det også logisk å benytte de samme aksesskontroll-mekanismene i alle tre tilfeller.

## Inn med 802.1X

**EAP** – Extensible Authentication Protocol

**EAPOL** – EAP over LAN

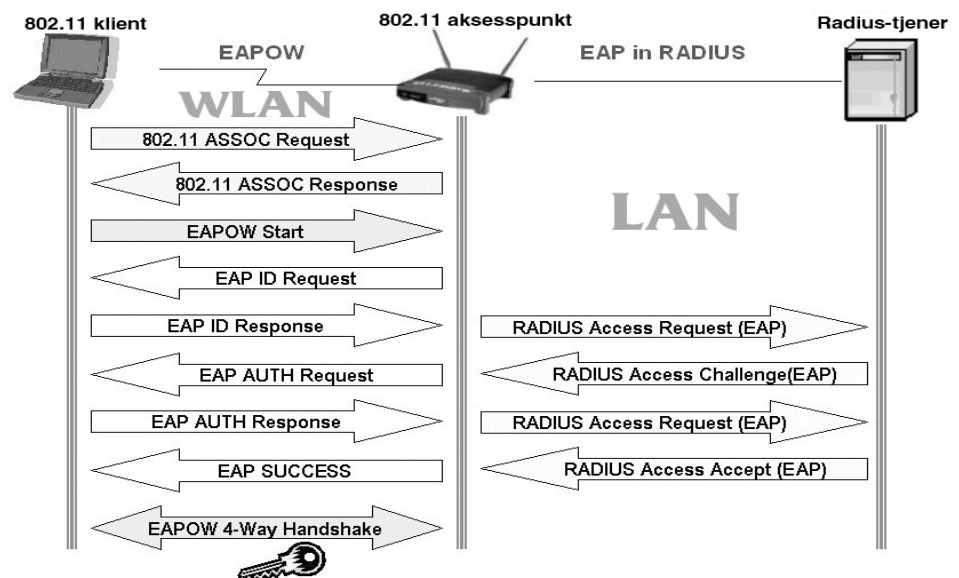
**EAPoW** – EAP over Wireless

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

802.1X-standarden, som ble ratifisert tidlig i 2003, angriper problemstillingene vi har gjennomgått ovenfor med en overraskende fokusering på enkelhet. Mekanismen kan sammenlignes med en av/på-bryter i svitsjen eller aksesspunktet. Bryteren blir slått på etter at autentiseringsprosessen er avsluttet med positivt resultat. Først da kan trafikk passere mellom klient og nettverk. Etter en avlogging eller *timeout* er vi tilbake til 'av', og trafikken blokkert.

802.1X definerer en lavnivå-protokoll for klientenes forespørsel om tilgang til nettverket. Protokollen tar utgangspunkt i en autentiseringsmekanisme som opprinnelig ble utviklet for oppringte samband – EAP. Mekanismen er tilpasset nye omgivelser for transport over Ethernet (EAPOL) eller trådløse forbindelser (EAPoW), og opererer på nivå 2 i nettverket – uten TCP/IP og IP-adresser. Å benytte en eksisterende protokoll i stedet for å 'finne opp hjulet på nytt' har tallrike fordeler i en slik setting. Ikke bare har mekanismen fått prøve seg i praksis over lang tid, og derigjennom fått luket bort svakheter. I tillegg har mange av leverandørenes programmerere allerede skaffet seg implementasjonserfaring, hvilket gir mer effektive og robuste implementasjoner og høyere grad av kompatibilitet leverandørene imellom.

En klient som skal autentiseres, må først komme i fysisk kontakt med nettverket – gjennom å plugges til et LAN eller komme innenfor rekkevidde av et WLAN. Med forbindelsen på plass, sender klienten avgårde en 'EAP Start' melding, som forårsaker en serie transaksjoner frem og tilbake – først mellom klient og aksesspunkt/svitsj og dernest mellom klient/svitsj og en bakenforliggende RADIUS-tjener, hvor den egentlige autentiseringen skjer. Prosessen avsluttes med enten en 'EAP Success' eller 'EAP Failure'. Her er det viktig å observere at selv om klienten for



**Figur 2**

En 802.1X-autentisering foregår mellom klient og tilkoblingspunkt på nivå 2 i nettverket. Først etter en vellykket autentisering får klienten 'fysisk tilgang' til nettverket innenfor – på IP-nivå (nivå 3). Mekanismen er den samme for kabelbaserte tilkoblinger, med unntak av den innledende assosiasjons-forespørselen og den avsluttende transaksjonen med krypteringsnøkler. [Figur fra wi-fiPlanet.com]

å kunne autentisere seg, må ha det vi tradisjonelt kaller fysisk tilgang til nettverket, stopper denne fysiske tilgangen ved svitsjen eller aksesspunktet. Det er her vår logiske av/på-bryter befinner seg. Klienter har ingen egentlig tilgang til nettverket før denne bryteren er åpnet.

Hvordan dette foregår er illustrert i figur 2, hvor vi også ser at det trådløse scenariet inneholder to ekstra transaksjoner – én før og én etter selve autentiseringen. Den første ser 'assosieringen', som alltid innleder tilkoblingen av en trådløs klient til et aksesspunkt. Her etableres den fysiske forbindelsen, tilsvarende å plugge kabelen i veggen for et LAN. Den avsluttende transaksjonen, som også er unik for WLAN, er tildelingen av en krypteringsnøkkel for den trådløse forbindelsen.

Sett fra et sikkerhetssynspunkt er denne spesielt viktig fordi den ivaretar en velkjent og signifikant svakhet ved WLAN i sin alminnelighet og spesielt WLAN som benytter WEP-kryptering. Statiske krypteringsnøkler som fordeles manuelt og er like hos alle klienter, gir bedre transportsikring enn ingen ting, men er tunge å administrere, vanskelige å forandre og skalerer dårlig. Med den oppdaterte utgaven av 802.1X<sup>9</sup> som benyttes i dag, distribueres krypteringsnøkklene automatisk avslutningsvis i autentiseringsprosessen, hvilket bidrar til en viktig heving av sikkerheten ved bruk av WLAN.

### **Enkelt – men det er utenpå ...**

Sammenligningen med en av/på-bryter tegner et bilde av 802.1X som en enkel og elegant løsning på denne delen av sikringsproblematikken. Mens begge adjektiver er korrekte, er det også et faktum at enkelheten raskt forsvinner når vi studerer hva som foregår på innsiden av selve autentiseringsprosessen.

Utfordringen er ikke å formidle transaksjonene, men å møte virkelighetens behov med hensyn til autentiseringsmekanismer – et mangefasettet troll med utallige varianter, krav, behov og fasetter. Mens noen bruker Smart-kort, Token-kort eller engangs-passord fra kalkulatorlignende 'duppedingser', satser andre på fingerscannere eller digitale sertifikater – og en stor gruppe lever fortsatt i en verden dominert av tradisjonelle passord. Denne floraen av varianter kan EAP-protokollen sørge for en effektiv og robust innkapsling av, mens den egentlige jobben utføres langt bak kulissene – av RADIUS-tjeneren.

### **Fortsettelse følger**

I neste utgave skal vi ta en rask titt bak disse kulissene for å gi et inntrykk av hvilken fleksibilitet som er innbakt i konseptet og hvilke parametre det er viktig å se etter når produkter skal anskaffes. Hvor stor er avstanden fra god idé til effektiv implementasjon av 802.1X? ■

<sup>9</sup> 802.1X benyttet først en enkel transaksjon for overføring av krypteringsnøkler. Denne viste seg å være 'kompromitterbar', og er i en oppdatert utgave (som for å gjøre forvirringen komplett kalles 802.1aa) erstattet av en fireveis transaksjon (FOUR WAY HANDSHAKE) som eliminerer risikoen.