

802.1X: THE INSIDE STORY

I forrige utgave presenterte vi 802.1X-standarden som en effektiv og standardisert vei til dekning av dagens behov for nettverksautentisering. Blant ingrediensene finner vi en rekke kjente standarder fra lignende sammenhenger, som i 802.1X er satt sammen på en måte som har vakt berettiget positiv oppmerksomhet både i tekniske miljøer og i markedet generelt.

Disse egenskapene har blant annet ført til at 802.1X-implementasjoner for lengst er blitt en selvfølge i nettverksutstyr – fra de rimeligste trådløse aksesspunkter til sofistikerte svitsjer, klientoperativsystemer og tjenere. Veien fra eksistens og tilgjengelighet til bruk er imidlertid ikke alltid like kort, spesielt i situasjoner der det allerede finnes hjelpemidler som tilsynelatende ivaretar behovene. At et bedre alternativ finnes er ikke tilstrekkelig til å få en forandring inn på prioriteringslistene. Dessuten er det med 802.1X som med de fleste nettverksrelaterte standarder: Den er full av valgmuligheter og opsjoner som medfører at utstyr som implementerer standarden ikke nødvendigvis spiller sammen.

Enkelt – men det er utenpå ...

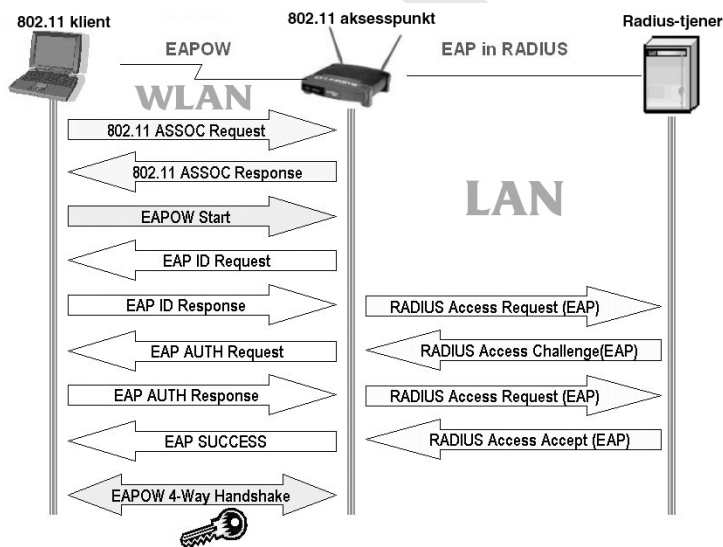
Mens 802.1X på utsiden karakteriseres av enkelhet og effektivitet, er innsiden det motsatte – en ikke uvanlig situasjon i teknisk sammenheng, med mikroprosessorer eller hovedkort som nærliggende eksempler. Som vi påpekte i forrige artikkel, er problemstillingene i utgangspunktet trivielle, og kan forenkles ned til en av/på-bryter ved den fysiske inngangen til nettverket. Virkeligheten mekanismene skal fungere i, er imidlertid alt annet enn enkel.

Med EAP i sentrum

Figuren nedenfor, som forklarer hvilke transaksjoner som er involvert i en autentiseringsoperasjon for en trådløs klient, illustrerer blant annet hvilken sentral rolle EAP – EXTENSIBLE AUTHENTICATION PROTOCOL – spiller i 802.1X.

EAPs historie går tilbake til første halvdel av 90-tallet, hvor den kom på banen som en nødvendig utvidelse av PPP-protokollen. Som navnet indikerer, er 'utvidbarhet' en av dens viktigste egenskaper, hvilket også er årsaken til at den stadig har funnet nye omgivelser å fungere i. I vår sammenheng sørger følgende virkelighetsbeskrivelse for å illustrere utfordringen:

Mens selve mekanismen som illustreres av figuren til venstre, er enkel nok å for-



stå, og blant annet viser at 802.1X konsoliderer autentiseringen til en RADIUS-tjener inne i nettverket, blir floraen av tenkelige og utenkelige klienter og brukergrupper en betydelig utfordring. Selv i et relativt homogent miljø finner vi typisk minst en håndfull ulike metoder for identifikasjon av klienter og brukere overfor nettverk og tjener-ressurser, fra tradisjonelle brukernavn/passord-kombinasjoner via Windows domene-pålogginger med CHAP som haleheng, til mer sofistikerte varianter med Smartkort og krypteringsnøkler.

Alle disse skal håndteres sømløst og sikkert av EAP innenfor rammene av 802.1X. Hvordan det skjer er uinteressant for brukerne, men viktig å ha kunnskap om for de av oss som skal mene noe om og sette i drift slike løsninger og mekanismer.

Under panseret

EAP – Extensible Authentication Protocol

TLS – Transport Layer Security

TTLS – Tunneled TLS

CHAP – Challenge Handshake Authentication Protocol

MS-CHAPv2 – Microsofts utgave av CHAP, versjon 2

PAP – Password Authentication Protocol

MD5 – En populær og rask énveis hash-funksjon for koding av meldinger, brukes mest for koding av passord.

Som figuren ovenfor viser, er tre parter involvert i autentiseringsprosessen: Klienten, aksesspunktet og autentiserings-tjeneren (vi holder oss til det trådløse eksemplet, det kan enkelt nok overføres til andre omgivelser ved behov). Det betyr ikke bare at alle tre må ha støtte for 802.1X, men at de må støtte den samme eller være kompatible med den samme versjonen av standarden. Dermed er den ene katten ute av sekken: 802.1X er ikke en 100% entydig betegnelse.¹¹ Dessuten må de støtte de samme autentiserings-metodene. EAP er 'bæreren' av transaksjonene, og kan – som vi var inne på ovenfor – formidle et tosifret antall varianter av autentiserings-forespørselen. Kravet er at alle tre parter i prosessen har et felles multiplum.

Fakta på bordet

En av årsakene til at det er viktig for IT-personer å ha kunnskap på dette nivå, er at vi som regel står overfor valg når 802.1X-basert autentisering skal settes i drift. De fleste klienter støtter flere EAP-varianter, mens ulike utstyrs-leverandører har forskjellig oppfatning av hva som er best/sikrest og prioriterer deretter. Dermed er det ingen selvfølge at brikkene passer sammen, om de aldri så mye støtter 802.1X-standardens.

Tabellen på neste side oppsummerer de viktigste karakteristika ved de mest brukte autentiserings-metodene, og utfyller beskrivelsen av hver enkelt variant nedenfor:

EAP-MD5 er den enkleste varianten, som lar RADIUS-tjeneren autentisere klienten gjennom å verifisere en MD5-koding av brukerens passord. Mekanismen er et akseptabelt valg i interne lokalnett der brukerne blir ansett som pålitelige og faren for sniffing eller andre former for angrep små. Dette er standardmekanismen som finnes i alle

¹¹ 802.1X ble i løpet av 2003 oppdatert til å benytte en såkalt 4-veis HANDSHAKE for utlevering av krypteringsnøkler til trådløse klienter, en endring som hever sikkerheten ved bruk av både WEB og WPA vesentlig. Det korrekte navnet på den oppdaterte standarden er 802.1aa, men den omtales like fullt som 802.1X. Utstyr som er levert i løpet av det siste året, støtter sannsynligvis den oppdaterte standarden.

Tabell 1 En rekke EAP-varianter er definert for å støtte ulike autentiserings-metoder og sikkerhets-regimer. Tabellen viser de mest vanlige. Se forklaringen på neste side og forkortelsene i margrammen for detaljer.

	LEAP	PEAP	EAP-TLS	EAP-TTLS	EAP-MD5
Autentisering av tjenersiden	Kodet passord ^a	Offentlig krypteringsnøkkel (fra digitalt sertifikat)	Offentlig krypteringsnøkkel (fra sertifikat)	Offentlig krypteringsnøkkel (fra sertifikat)	Ingen
Autentiseringen av klient	Kodet passord	Valgfri EAP-variant, f.eks. EAP-MS-CHAPv2 eller offentlig krypteringsnøkkel fra sertifikat	Offentlig krypteringsnøkkel (fra sertifikat eller Smartkort)	CHAP, PAP, MS-CHAPv2, EAP	Kodet passord
Formidling av dynamiske krypteringsnøkler	Ja	Ja	Ja	Ja	Nei

^a Et 'kodet passord' (PASSWORD HASH på fagspråket) er et passord som har fått en elementær form for kryptering via en såkalt hash-algoritme. Å sende et kodet passord over nettet er vesentlig sikrere enn å bruke klartekst, men slik koding er – av matematiske årsaker aldri spesielt sikker. Særlig hash-algoritmene som brukes i Windows er utsatt, fordi det finnes utallige fritt tilgjengelige verktøy for å knekke dem.

RADIUS-tjenere. Den er ikke egnet for offentlige nett, uavhengig av kategori eller teknologi.

LEAP utvider funksjonalitet og kvalitet i EAP-MD5 (ovenfor) med gjensidig autentisering av både klient- og tjenersiden, og formidling av nøkler for kryptering i WLAN. LEAP er utviklet av Cisco og mest utbredt i Cisco-dominerte miljøer som ønsker en snarvei til bedre WLAN-sikkerhet. Den er ikke egnet for offentlige nett, blant annet fordi passordene fortsatt er kodet, ikke krypterte.

PEAP (Protected EAP) og EAP-TTLS (EAP med TLS i tunnel) foreligger som standardforslag (PEAP fra Cisco og Microsoft, EAP-TTLS fra Funk Software) hos Internettets standardiseringsorgan IETF, og har til hensikt å forenkle utrulling av 802.1X. Begge forutsetter sertifikat-basert autentisering av RADIUS-tjeneren, mens klientautentiseringen er fleksibel. Organisasjoner som ikke har utstedt digitale sertifikater til hver bruker/klient og ikke ønsker å gjøre dette kun for å komme i gang med 802.1X, kan bruke Windows brukernavn og passord i stedet. En RADIUS-tjener som støtter EAP-TTLS og PEAP kan kontrollere autentiserings-forespørsler mot Windows domene-kontrollere, Active Directory-tjenere eller andre brukerkataloger. Robustheten mot sniffing er den samme som for EAP-TLS (se nedenfor), men sikkerheten er ikke like god siden passord kan gjettes eller skaffes på andre (ikke-tekniske) måter.

EAP-TLS (EAP med Transport Layer Security) ble etablert som standard allerede i 1999, og er den eneste fullt standardiserte mekanismen for sikker autentisering i trådløse nettverk i dag. EAP-TLS forlanger at både klient og RADIUS-tjener autentiseres via digitale sertifikater eller Smartkort (offentlige krypteringsnøkler). Transaksjonen er sikret ved hjelp av en kryptert TLS-tunnel, hvilket gjør den motstandsdyktig mot de fleste former for angrep. Det er imidlertid fortsatt mulig å sniffe seg til klientenes identiteter, som gir et utgangspunkt for

videre angrepsforsøk, teknisk eller sosialt. Mekanismen er mest attraktiv for større organisasjoner som kun kjører Windows og som har utstedt digitale sertifikater til brukerne.

Fra teknologi til produkter

Hvilke konklusjoner kan vi trekke av dette? Hvem støtter hva og hvorfor, og hva er optimalt for oss? Det kommer naturligvis an på hvem som spør: Hvilke leverandører som er dominante i et gitt miljø vil alltid gi en pekepinn om hvilket alternativ som er enklest å sette i drift. Hva som er sikrest, er som regel en annen sak. Tabellen nedenfor gir en pekepinn om hvem som støtter hva.

Tabell 2 Oversikt over hvilke leverandører og plattformer som støtter hvilke EAP-varianter. Husk at dette er dynamisk informasjon som forandrer seg fra én versjon til den neste av produktene.

	LEAP	PEAP	EAP-TLS	EAP-TTLS
Leverandører hvis RADIUS-tjenere støtter mekanismen	Cisco, FreeRADIUS, Funk, Interlink, Meetinghouse, Radiator	Cisco, Microsoft, Funk, Interlink, Meetinghouse, Radiator	Cisco, Microsoft, Funk, Interlink, Meetinghouse, Radiator, FreeRADIUS	Funk, Interlink, Meetinghouse, Radiator
Leverandører av klientstøtte	Cisco, Funk, Meetinghouse	Funk, Meetinghouse, Microsoft	Cisco, Funk, Meetinghouse, Microsoft, Open1X	Alfa-Ariss, Funk, Meetinghouse, Open1X
Støtte inkludert i OS		Windows XP, 2000, 2003	Windows XP, 2000, 2003	
Plattformer støttet av 3-part	Win32	Win32	MacOS-X, BSD, Linux, Win32	MacOS-X, BSD, Linux, Win32

De fleste leverandørene av RADIUS-tjenere forsøker naturligvis å levere maksimal funksjonalitet i et voksende marked. Generelt har EAP-TLS bredest støtte – av naturlige årsaker, men som tabellen viser er det ikke vanskelig å finne produkter som støtter andre alternativer. Den viktigste utfordringen er å sørge for at RADIUS-tjeneren, aksesspunktene og klientene (og kantsvitsjene, dersom LAN-brukere skal autentiseres) er kompatible. Sjekk at både 802.1X-versjonen og EAP-mekanismen er støttet av alle. Videre, dersom PEAP benyttes, må det kontrolleres at den valgte autentiseringsmekanismen har støtte i alle ledd. Microsoft og Cisco har distribuert ulike og inkompatible implementasjoner av nettopp PEAP.

Klienter, skalering og utfordringer

Mer sikkerhet i Mellvik-Rapporten

I 1. kvartal 2005 skal vi blant annet innom Open Source verktøyene FreeRADIUS og Open1X, som begge er relevante i tilknytning til 802.1x og WLAN-sikkerhet.

Den største utfordringen er – knapt overraskende – å finne på klientsiden: Installasjon og konfigurering av klient-programvare og brukernes sertifikater. Vi oppsummerer en samling gode råd i den forbindelse i fire punkter som er å finne i tilleggstoffet til denne utgaven på vår Web-tjeneste. På samme side vil du også finne praktiske hint om utrulling av 802.1X – en øvelse som ikke bare er krevende i forbindelse med produktvalg, men som samtidig skal kombineres med andre sikringstiltak for å gi optimale resultater.

Direkte-koblingen til denne websiden er www.mellvik.no/MR122. ■