

Wireless Ethernet: Et åpent sikkerhetshull?

Selv i vår lokale andedam får sikkerhet og trådløse nettverk betydelig oppmerksomhet i disse dager – ikke bare på grunn av stor vekst og ivrige leverandører. Hackere og andre interesserte har kastet sine øyne på denne relative nykommeren, og kjører rundt i områder med kontorbygg der de kobler seg på nettverkene tilsynelatende uten hindringer av noe slag. Det samme skjer i Stockholm, London og San Francisco. Kan situasjonen virkelig være så ille som den beskrives? Representerer de trådløse nettverkene enda en ukontrollerbar trussel, gigantiske hull i velutviklede forsvarsverk?

Med den eksplosive utvikling trådløse nettverk opplever, er problemstillingen hyper-relevant. Vi setter søkelyset på svakhetene, mulighetene og realitetene: Hvor ille er det, hva kan og bør vi foreta oss og hvilke utsikter finnes til å redusere eller eliminere de problemene som åpenbart finnes?

Storm i vannglass?

I første omgang er det fristende å kalle oppstyret for storm i et vannglass. Nå er imidlertid sikkerhet et altfor viktig tema til å kimses av. Det faktum at situasjonen i mange tilfeller er så ille som pressen forteller, indikerer at noe er galt. At problemet ikke nødvendigvis har med produktene å gjøre er en annen sak. Som Mellvik-Rapportens lesere er særdeles klar over, etableres sikkerhet kun i beskjeden grad gjennom installasjon av apparater, mekanismer og programvare (se for eksempel artikkelen “Brannmurer: Mye penger, lite sikkerhet” i Mellvik-Rapporten nr. 57⁷).

I forrige utgave (nr. 83 side 30) påpekte vi at samtlige WE-produkter på markedet leveres med sikkerhetsmekanismer som kan aktiviseres med et enkelt håndgrep. Disse mekanismene er en del av WE-standarden, og går under betegnelsen WEP – *Wired Equivalent Privacy*, et navn som danner et godt utgangspunkt for å skape riktige forventninger.

WEP

WEP er en protokoll og en algoritme – krypteringsmatematikk for viderekomme – som karakteriseres av et fåtall parametre som vi skal komme tilbake til nedenfor. Som navnet sier, er målsettingen å etablere grunnleggende sikring, slik at forbindelser via eteren kan få omtrent samme sikkerhetsnivå som kabelbasert trafikk. Eksistensen av WEP impliserer en erkjennelse av at trådløse nettverk per definisjon er mer utsatte enn sine kabelbaserte slektninger. Dette til tross for at de fleste kabelbaserte nettverk også kan avlyttes trådløst. Riktignok kreves det mer sofistikert utstyr enn tilfellet er for WE, der alt vi tren-

⁷ Utgaven er tilgjengelig ON LINE fra vår Web-tjeneste.

ger er et PC-kort fra butikken på hjørnet for å sette i gang. På den andre siden er trafikken i det kabelbaserte nettverket som regel åpen og ukryptert, slik at den er lett å forstå når tilgangen er et faktum.

Hvorvidt et kryptert trådløst nettverk er like sikkert eller usikkert som et kabelbasert nett, kommer med andre ord an på to faktorer: Hvor fysisk lett tilgjengelig det kabelbaserte nettverket er, og hvor god krypteringen av den trådløse trafikken er. Når vi evaluerer sikkerheten i et trådløst nettverk, er det med andre ord nødvendig å ta vare på bakkekontakten – slik at kravene står i forhold til andre alternativer. Å forkaste trådløse nettverk på sikkerhetsmessig grunnlag, blir meningsløst dersom vi aksepterer kabelbaserte nettverk med samme sikkerhetsnivå. Dessuten finnes det alltid muligheter for tilleggssikring, uansett fysisk nettverk og transportteknologi.

Kryptering med variasjoner

Forutsetning nummer én for grunnleggende sikkerhet i et trådløst nettverk er kort og godt at de 'medfødte' mekanismene er aktiviserte. Neste spørsmål blir da hvor gode de er – kvalitativt og implementasjonsmessig, og hvor compatible de er på tvers av plattformer. Lenger trenger vi ikke å gå for å befinne oss i et ormebol av ulike meninger og synspunkter fra eksperter og produktutviklere.

Ekspertene angriper

Mens hovedårsaken til den negative publisiteten vi har sett de siste månedene, har sin årsak i likegyldighet eller inkompetanse hos de som er ansvarlige for installasjonen, er det også kommet frem til dels krass kritikk mot matematikken som er valgt i 802.11b-standarden (WEP). Forskere fra Universitetet i Berkeley, California går spesielt kraftig ut, og trekker følgende konklusjon i et dokument der en håndfull angrepsmetoder med varierende innsats blir påvist å lykkes:

Wired Equivalent Privacy (WEP) isn't. The protocol's problems are a result of a misunderstanding of some cryptographic primitives and therefore combining them in insecure ways. These attacks point to the importance of inviting public review from people with expertise in cryptographic protocol design; had this been done, the problems stated here would surely have been avoided.
[www.isaac.cs.berkeley.edu/isaac/wep-faq.html]

Kritikken går med andre ord to veier: At WEP-protokollen er et resultat av dårlig håndverk, og at prosessen bak etableringen av standarden burde ha vært mer åpen. Her er det standardiseringsorganisasjonen IEEE som angripes, og som seg hør og bør har Stuart J. Kerry, leder for gruppen som arbeider med nettopp dette området, tatt til motmæle. Utover å forsvare arbeidet som er gjort, fører han i marken to poenger som er verdt å legge merke til:

- ✓ Han påpeker at sikkerhet og sikring er relative begreper og at enhver algoritme kan knekkes gitt tilstrekkelige ressurser.
- ✓ Videre hevder han at standardiseringsprosessen i IEEE (*Institute of Electrical and Electronics Engineers*) er fullstendig

åpen og at hvem som helst kan delta, kritisere og bidra hele veien.

Mens begge punktene teknisk sett er korrekte, bidrar spesielt den siste til å øke forvirringen i stedet for det motsatte. Forskerne mener at algoritmen med små forandringer kunne ha vært av vesentlig bedre kvalitet – i praksis mye vanskeligere å knekke. Dette er åpenbart viktig fordi vi uten tilleggs kostnader ville ha fått betydelig bedre sikkerhet. Med hensyn til prosessen, er kritikken høyst relevant: Hvem som helst kan riktignok delta i IEEE-prosessene, men må være til stede *in person* på møtene, og må kjøpe dokumentene som er involvert. De er kostbare – typisk et par hundre USD per dokument. Kritikerne mener at dette gjør åpenheten til en vits, og at organisasjonen burde legge om rutinene og derigjennom heve kvaliteten på arbeidet som gjøres.

Erfaring fra Internett-miljøene gjennom 30 år, og fra ulike Open Source prosjekter de siste 10-15 årene, levner ingen tvil om at en fullstendig åpen prosess, gir nettopp slike resultater.

Kritikken og resultatene fra Berkeley kan med andre ord ikke ignoreres av IEEE, som uten å innrømme noen feil har satt ned en gruppe for å undersøke saken nøyere. Dette vil ta tid – som slike prosesser alltid gjør, og veien frem til en eventuell ny utgave av standarden er lang og kronglete. Videre er det ingen selvfølge at en endret standard vil føre til endrede produkter innen overskuelig tid. Dermed blir det mer interessant for oss som skal bruke – og ta ansvaret for – dagens produkter, å spørre: Hvor ille er situasjonen, hva kan vi gjøre og hva bør vi absolutt ikke gjøre?

Fra teori til virkelighet

Svakhetene som er påvist i WEP-protokollen berører alle Wireless Ethernet-produkter, og er ikke til å kimse av. Bedre blir det naturligvis ikke av vår ervervede kunnskap om at situasjonen lett kunne ha vært meget bedre. På den andre siden er dette også *business as usual*. Alle tenkelige protokoller har sikkerhetsproblemer i varierende grad – som på et eller annet tidspunkt blir oppdaget, og som dermed taper respekt hos eksperter og marked.

Dette kan ved første øyekast virke logisk: Før feilene eller svakhetene er oppdaget, blir produktet/protokollen/teknologien betraktet som relativt sikker, mens den etterpå blir stemplet som det motsatte. Ved nærmere ettertanke ser vi at dette er å snu tingene fullstendig på hodet: Før svakheten blir offentlig kjent, er usikkerhetsfaktoren stor fordi ingen egentlig vet hvem – om noen – som kjenner til og er i stand til å utnytte kunnskapen. Så snart den blir offentlig, er det mulig å gjøre noe med forholdet, enten gjennom å forandre produktet, eller gjennom andre tiltak. Sagt på en annen måte: *Security through obscurity* er en like dårlig idé i denne som i de fleste andre sammenhenger.

Videre kan vi nok en gang observere den evige sannhet at design av sikkerhetsmekanismer og protokoller er komplisert og krevende. Det forekommer aldri at de blir riktige eller optimale i første runde. Derfor

er det av stor betydning å sørge for at design-prosessen blir så åpen og tilgjengelig som mulig: Flere øyne gir færre feil og bedre resultat.⁸ Vi ser også at slagord og salgsargumenter ofte har lite med reell sikkerhet å gjøre. I brosjyrene for de fleste Wireless Ethernet-produktene på markedet kan vi lese at sikkerheten er ivaretatt med en "128 bits RC4"-algoritme. Mens dette høres fint ut, viser erfaringene vi har referert ovenfor at ord er billige og forteller lite om den reelle sikkerheten.

Det svakeste ledd ...

Dessuten er det både viktig og nødvendig å plassere elementene i et riktig perspektiv: WEPs svakheter er behørig dokumentert, men hvilken rolle spiller de dersom andre ledd i sikkerhetskjeden er enda svakere? Årsaken til de store avisoppslagene om WE og sikkerhet den siste tiden har, som vi har påpekt, sin årsak i slendrian hos de ansvarlige.

Dessuten – og helt uavhengig av WEPs kryptografiske egenskaper, benytter WE en autentiserings-mekanisme som er passordbasert: De som kjenner passordet, får tilgang til nettverket. Passordet fungerer både som adgangskode og som nøkkel til krypteringen, og er i de fleste tilfeller likt – ikke bare for alle klientene, men også for samtlige basestasjoner – for å gi brukerne mobilitet ('roaming'). Det legges inn sammen med driveren, og ligger lagret på alle klienter – og aksesspunkter – uten å være spesielt sikret på noen måte. Videre byttes dette passordet praktisk talt aldri etter at de er lagt inn. Det er rett og slett for komplisert i og med at hver enkelt klient må forandres.

Sikkerheten blir deretter. Det skal ikke mer enn et utlån, et tap av en PC eller en oppsagt medarbeider til for å gjøre den lille passordhemmeligheten til offentlig kunnskap. Da spiller det liten rolle hvilken algoritme som benyttes og hvilke kvaliteter og svakheter den måtte ha.

Aksesskontroll

Utover kombinasjonen passord/krypteringsnøkkel, har WE-produktene en funksjon som kalles SSID, *Service Set ID*, et slags nodenavn for hver basestasjon. Når den aktiviseres, må klienter oppgi riktig navn for å få tilgang til en gitt basestasjon. Mekanismens primære hensikt var å gjøre det mulig for brukergrupper å 'reservere' en basestasjon, mens det i praksis blir brukt som aksesskontroll. Noen stor effekt har den ikke, siden alle klienter deler samme ID, men den forhindrer tilfeldige 'forbipasserende' i å knytte seg opp mot nettverket.

Videre har de fleste WE-produkter på markedet støtte for såkalte aksesslister: Lister med lavnivå- (MAC-) adresser som er akseptable for den enkelte basestasjon. Med automatiske mekanismer for oppdatering, er dette en overkommelig og effektiv sperre mot tilfeldige 'sniffere' som gir bedre beskyttelse enn SSID. Samtidig er det viktig å være klar over begrensningene:

⁸ Dette er en av grunn-tesene for kvaliteten vi i dag finner i OPEN SOURCE SOFTWARE, formulert av Eric S. Raymond – blant annet i boken "The Cathedral and the Bazaar".

- ✓ Det er relativt enkelt å forandre MAC-adressen på et Ethernet-kort i driveren. Klarer en inntrenger å skaffe seg en akseptert adresse, er det med andre ord lett å bruke den.
- ✓ MAC-adresser er som regel trykket på undersiden av PCMCIA-kort. Dermed kan spesielt interesserte med beskjeden innsats skaffe seg tilgang til dem.
- ✓ Enkelte produkter har sterke begrensninger i antall MAC-adresser som kan legges inn i en aksessliste. Dette kan gi skaleringsproblemer.

Neste trinn

Når standardene ikke strekker til, går leverandørene gjerne sine egne veier, og WE representerer intet unntak i så måte. Alternative krypteringsalgoritmer og metoder for aksesskontroll dukker stadig opp, og er uten unntak proprietære i den forstand at de kun virker når klienter og basestasjoner kommer fra samme leverandør.

Enkelte fellestrekk har de imidlertid – spesielt med hensyn til autentisering: En standard for autentisering i lokalnett, uavhengig av underliggende transport-teknologi, er under arbeid i IEEE, med navnet 802.1x. Den tar utgangspunkt i RADIUS (*Remote Authentication Dial-In User Service*), som er en Internett-standard (se Mellvik-Rapporten nr. 56), og vil etablere et nytt nivå for autentisering og dermed sikkerhet i nettverk generelt og for WE spesielt.

Standarden vil imidlertid i beste fall bli klar til kommende årsskifte, med samspillende produkter tilgjengelige om ca. et års tid. I mellomtiden er vi henvist til enten proprietære eller alternative løsninger dersom vi ønsker sikkerhet utover det nivå WE gir.

Alternativer

Det innlysende alternativet som praktisk talt eliminerer alle disse svakhetene og utfordringene, er naturligvis å benytte VPN-teknologi. Ved å forlange at alle trådløse klienter kobler seg opp mot lokalnettet via en VPN-forbindelse som både gir autentisering av brukeren og kryptering av datastrømmen, er de fleste bekymringene vi har nevnt ovenfor borte. Vi kan sågar fjerne WPE-krypteringen dersom den representerer en merkbar forsinkelse i trafikkavviklingen uten konsekvenser for sikkerheten for den løpende trafikk. Det betyr imidlertid ikke at WEP gjøres verdiløs av VPN: Den bidrar fortsatt til å hindre uvedkommende i å få forbindelse med nettverket, og reduserer dermed sjansene for driftsforstyrrelser.

I et større nettverk med mange aksesspunkter kan det også være hensiktsmessig å segmentere ut all WE-trafikk til et eget logisk nettverkssegment, hvilket er mulig med svitsjer som støtter 802.1Q VLAN-protokollen.⁹ På den måten får vi kontroll over grensepasseringene

⁹ Status for VLAN-teknologi generelt og 802.1Q-protokollen spesielt blir diskutert i en egen artikkel i Mellvik-Rapporten i 2. halvår i år.

mellom det trådløse og det interne nettverket, hvilket alltid er en stor fordel med hensyn til såvel sikkerhet som kontroll og styring.

Konklusjon

Sikkerhetsrisikoer finnes over alt, og trådløse nettverk hører til en kategori som krever spesiell oppmerksomhet – fordi eksponeringen blir stor dersom ingen ting gjøres.

Vi har konstatert at WEP verken gir god sikkerhet eller autentisering, med den følge at Wireless Ethernet aldri bør installeres uten en grundig evaluering av sikkerhetsmomentene. 100% sikkerhet finnes ikke, og her som ellers må sikkerheten kvantifiseres og kvalifiseres i forhold til hva som skal beskyttes.

Sine feil og mangler til tross, er WEP slett ikke verdiløs, men gir moderat sikkerhet – og var laget med et slikt mål for øyet. I ekspertenes øyne kan WEP se ut som en feiltagelse, men det er også verdt å huske at IEEE har hatt flere enn de sikkerhetsmessige sidene å ta hensyn til i forbindelse med utviklingen. For eksempel var det viktig å finne en krypteringsalgoritme som ikke ble rammet av amerikanske eksportrestriksjoner. Videre skulle det legges til rette for kompromisser på hardware-siden som holdt produktkostnadene nede og ytelsen oppe.

Vi kan med andre ord kritisere oppad stolpe og nedad vegg, men faktum er at vi fortsatt har anledning til å etablere så god sikkerhet som vi ønsker. At ikke alle mekanismene er innebygget i transport-teknologien kan like gjerne være en fordel som en ulempe. For eksempel er det en god vane å benytte VPN for alle mobile brukere, uansett om de er utenfor eller innenfor organisasjonens kontorer. Å fjerne sikringen fra transportnivå blir dermed en forenkling i stedet for en komplikasjon: Samme sikkerhetsmekanisme uansett forbindelsestype.

Praktiske leveregler

I praksis er følgende sett av regler nyttige i forbindelse med sikring av trådløse lokalnett:

- ✓ Sikkerhetsmekanismene som finnes må aktiveres! Å idriftsette et system uten noen form for sikring er oppsigelsesgrunn – eller grunnlag for søksmål mot en leverandør – for skjodesløshet.
- ✓ WEP gir moderat, men ikke god sikkerhet. Det trådløse nettverket må behandles deretter. Mye kan sies om WEPs svakheter, men at den hever vanskelighetsgraden for inntrenging og misbruk betraktelig, er et faktum.
- ✓ De fleste produkter støtter både 40/64 bits RC4 og 104/128¹⁰ bits RC4 kryptering. Velg alltid den kraftigste krypteringen. Dersom dette går merkbart ut over ytelsen, er utstyret (basestasjonene) for svakt og bør byttes ut. Flere tester har avslørt at det er betydelige forskjeller mellom produk-

¹⁰ 24 bits brukes som identifikator, mens de resterende representerer krypteringsnøkkelen.

Vi kommer også inn på sikkerhetsaspekter knyttet til Wireless Ethernet i neste utgave, i artikkelen om neste generasjons WE (se baksiden).

tene på markedet i så henseende. Se etter produkter som foretar kryptering i hardware.¹¹

- ✓ Aksesslister (bestående av gyldige MAC-adresser) gir ytterligere sikring og aksesskontroll, og er ukomplisert i små nettverk. Bruk av proprietære mekanismer – gjerne med RADIUS i bakkant – er også et alternativ, selv om det gir binding til én spesifikk leverandør, permanent eller midlertidig.
- ✓ Rutiner for forandring av 'passordet' må etableres.
- ✓ Der god sikkerhet er et krav, brukes VPN over WE.
-

¹¹ Ytelseeffekten av kryptering påvirker ikke bare aksesspunktene. Datastrømmen skal krypteres på klientsiden, hvilket kun unntaksvis gjøres i sin helhet av hardware (PC-kortet). Derfor viser det seg at gamle – og svake – PCer kan forårsake merkbare forsinkelser når 128 bits kryptering benyttes.