

WLAN: Det du ikke vet, har du vondt av

“Visst har vi sikret det trådløse nettverket. Vi bruker kryptering, forlanger alltid autentisering og sørger for at trafikken behandles av brannmur som om den var ekstern. Nei, vi bruker ikke WPA, det ble for komplisert med Windows 2000, så vi ble nødt til å velge WEP. Og det er vesentlig bedre enn ingen ting. Nei, vi har ikke satt i drift 802.11i enda, slikt tar tid. 802.11i og WPA står på kjøreplanen – når vi får tid.”

Litt sikkerhet er bedre enn ingen ...

Kjenner du deg igjen? Det er ingen skam å innrømme det, og du er i så fall i godt selskap. Oppsummeringen gjelder for de fleste små og mellomstore miljøer – og indikerer på den ene siden at WLAN-sikring er inne på radaren, og på den andre siden at forbedringspotensialet er betydelig.

Den generelle bevisstheten omkring risikomomentene knyttet til trådløse nettverk har sørget for en dramatisk reduksjon i antall fullstendig åpne og ubeskyttede nettverk, og samtidig fungert som en effektiv brems på idriftsettelsen av nye nettverk. En rekke undersøkelser både her hjemme og internasjonalt de siste 2 årene, bekrefter at sikkerhet fortsatt er den viktigste innvendingen mot bruk eller utvidelser av WLAN – fra såvel tekniske som ikke-tekniske personer.

... men kun god sikkerhet er tilstrekkelig

Mens denne bevisstheten er positiv og viktig, er den ikke tilstrekkelig til å gjøre WLAN til en sikker og pålitelig del av vår infrastruktur. Dessuten har vi med et bevegelig mål å gjøre – som beveger seg enda raskere enn andre sikkerhets-relaterte områder. Og sist, men ikke minst er trådløst utstyr og teknologi så billig, lett tilgjengelig og utbredt at terskelen for en ‘inntrenger’ eller ‘misbruker’ er minimal. Med PCer, mobiltelefoner, PDAer og annet utstyr fulle av WLAN-teknologi, skal det dessuten kun en porsjon skjodesløshet eller uvitenhet til fra brukerens side før infrastrukturen er helt eller delvis åpen for hele verden.

Det klassiske eksemplet er brukeren som installerer sitt eget aksesspunkt på kontoret for å slippe å koble kablen til sin nye bærbare. Denne muligheten har fått tilstrekkelig oppmerksomhet i media og fagfora til at alle som følger med, har sørget for å blokkere muligheten – for eksempel gjennom kontinuerlig kontroll med hvilke noder som er aktive og tillatte på nettverket. Et slikt tiltak berører imidlertid kun toppen av isfjellet. Her er en samling andre utfordringer knyttet til nettopp den lette tilgjengeligheten av sofistikert utstyr og tilhørende programvare:

- ✓ En PDA eller laptop med WLAN-grensesnitt og fritt tilgjengelig programvare (se tabellen på side 7) er alt som skal til for å

skaffe seg oversikt over hvilke muligheter eteren i nærmiljøet har å by på. Denne trusselen kan kun møtes ved å bruke de samme mekanismene til kontroll og beskyttelse.

- ✓ Enhver node med WLAN-grensesnitt er også et potensielt aksesspunkt. Feilkonfigurasjoner og mangelfull oppfølging (og såkalt brukervennlige innstillinger i operativsystem og drive-re), sørger for at en interessert forbipasserende kan få tilgang til brukerens utstyr, og enten kan tappe dette direkte eller bruke det som inngangsport til et bakenforliggende nettverk.
- ✓ Avlytting av trådløse nettverk kan – med gode antenner – gjøres flere hundre meter unna nærmeste basestasjon. Gode antenner kan også brukes til det motsatte – å blokkere nettverket ved å sende ut kraftige støysignaler etter god, gammel-dags østeuropeisk oppskrift (DoS, *Denial of Service* angrep).
- ✓ Når en klient kobler seg opp mot en trådløs basestasjon, vil den første del av transaksjonen ofte være åpen. For offentlige IP-soner og *hotspots* er dette sågar en nødvendighet. Det betyr at en avlytter kan kartlegge og kopiere i alle fall deler av denne oppkoblingssekvensen. Kunnskapen kan i sin tur brukes til å introdusere falske aksesspunkter som snapper opp klientforbindelsen og lurer brukeren til å autentisere seg. En slik sjanghaling kan gjennomføres uten at brukeren merker det, og vil i det minste gi inntrengeren informasjon om infrastrukturen og brukerens navn/passord. I verste fall kan hele sesjoner tappes på denne måten.

Spesielt siste punkt aksentuerer viktigheten av tosidig autentisering, som 802.1x-standarden introduserer (Mellvik-Rapporten nr. 121) og som suppleres av 802.11i (Mellvik-Rapporten nr. 120). **Bruk av mekanismene disse to standardene spesifiserer, er en forutsetning for god WLAN-sikkerhet.**

Ikke bare WLAN

Mens vi i denne artikkelen kun tar for oss WLAN, er det naturlig å minne om at en rekke av problemstillingene er analoge for Bluetooth, et forhold vi diskuterte i forrige utgave. Dersom Bluetooth fortsetter å utvikle seg i den retning som avtegner seg i dag, vil problemstillingene bli sterkt aksentuert i de neste to årene, et forhold det er all grunn til å ta på alvor allerede nå.

Full krig

Som vi var inne på innledningsvis, er imidlertid heller ikke 802.11i tilstrekkelig for å opprettholde det vi kan kalle god sikkerhet. I likhet med sikkerhet generelt, er det vi ikke vet om våre egne svakheter, ofte vår største svakhet. Det vi ikke vet, er det store sjanser for at noen andre har hel eller delvis kunnskap om. Dermed er vi tilbake til det gamle ordtaket om at *if you can't beat them, join them*.

Vi – eller de vi har delegert ansvaret til – må vite hvilke trusler som finnes og hvordan de kan brukes mot oss. Det betyr blant annet praktisk kunnskap om verktøy som er tilgjengelige for formålet, og som i de

Om lettvinhet, ad-hoc og trusler

De fleste organisasjoner forbyr – eksplisitt eller implisitt – bruk av ad-hoc nettverk, det vil si at brukerne kobler seg opp mot hverandre for spontan utveksling av data. Et slikt forbud er viktig, fordi utstyr som tillater ad-hoc oppkoblinger er lette mål for 'tilfeldige forbigående'.

Lettvinhet er imidlertid en uforutsigbar motstander for alt sikkerhetsarbeid. For eksempel vil en bruker som er på farten og har behov for å utveksle data på et møte eller kanskje med en annen maskin hjemme, gjerne aktivisere ad-hoc muligheten – i effektivitetens navn. Når transaksjonen er gjort, glemmes innstillingen, og utstyret blir fritt vilt frem til den igjen endres. I mellomtiden har maskinen gjerne vært innom både det ene og det andre nettverket, og hatt mulighet til å legge igjen virus, trojanske hester, eller rett og slett fungert som åpen port til intern infrastruktur.

Den eneste pålitelige måten å unngå slike situasjoner på, er å blokkere muligheten for bruk av ad-hoc innstillingen eller å avvise oppkobling fra utstyr som har denne innstillingen aktiv. Begge deler krever programvare som løpende kontrollerer klientutstyret.

fleste tilfeller er fritt tilgjengelige på Internettet. En rekke av verktøyene er laget for drifts-, sikrings- og kontroll-formål, men fungerer like godt i inntrengeres hender. På samme måte har vi i sikringssammenheng stor nytte av en rekke verktøy som utelukkende er laget for å avdekke og/eller angripe potensielle 'ofre'. Denne dualiteten er naturlig og finnes over alt rundt oss. En sivilisasjon uten kniver er utenkelig, men kniver er også våpen.

En flora av verktøy

Tabellen på neste side oppsummerer egenskapene til de viktigste verktøyene i klassen. Det er ingen tilfeldighet at samtlige hører hjemme i kategorien Open Source. Deling av kode, idéer, drivere og så videre er like viktig for inntrengere som forsvarere, og sørger for

at det ikke finnes særlig mange hemmeligheter på verken den ene eller den andre siden. De få kommersielle verktøyene som finnes i denne kategorien, tilfører lite på den funksjonelle siden, men kan kombineres med driftstjenester som gjør dem interessante for store miljøer.

Kvaliteten og brukervennligheten enkelte av disse verktøyene tilbyr – spesielt NetStumbler og Kismet, representerer en betydelig trussel i seg selv. Kombinert med GPS-informasjon kan disse verktøyene kartlegge store områder på kort tid, praktisk talt uten at 'operatøren' har teknologikompetanse. Desto viktigere er det at våre sikkerhetsansvarlige både er kjent med og benytter de samme verktøyene. Ikke minst med utgangspunkt i data fra disse to, kan vi finne flere oversikter over tilgjengelige aksesspunkter fra hele verden på Internettet, for eksempel www.wigle.net og www.wifinder.com. Å finne sin egen organisasjon på en av disse listene, er et klart signal om at tiden er overmoden for handling.

Falsk sikkerhet

Det faktum at WLANs alltid kan avlyttes er den innlysende årsaken til at de også er notorisk utsatt. At trafikken er kryptert forhindrer ikke at hvem som helst kan avlytte og lagre dataene som flyr gjennom eteren. Å lagre en kryptert datastrøm er riktignok i utgangspunktet meningsløst, men med tilstrekkelig mange dataenheter tilgjengelige kan et analyseprogram finne krypteringsnøkkelen for en hvilken som helst WEP-sikret forbindelse. Det skal fortsatt et milliontall pakker til – hvilket ikke tar mer enn en time eller to på et nett med beskjedent belastning. Denne virkeligheten illustrerer hvilken beskjedent verdi WEP-sikkerhet egentlig gir. Bedre enn ingen ting – uten tvil, men det er vanskelig å finne omgivelser utenfor privatmarkedet hvor WEP kan kalles 'godt nok'.

Underlig nok finnes det fortsatt mange som lever i den villfarelse at filtrering på MAC-adresse er en nyttig sikkerhetsmekanisme. Dette er i beste fall naivt – gitt hvor lett det er å lytte seg frem til aktive (godkjente) adresser og å endre sin egen. Dersom WEP-sikkerhet kalles en illusjon, blir MAC-filtrering for en spøk å regne i en slik sammenheng.

Tabell 1 Oversikt over Open Source-verktøy som benyttes i forbindelse med angrep på og beskyttelse av trådløse nettverk. Merk at mange av verktøyene har spesielle krav med hensyn til hvilke trådløse brikkesett som støttes. Listen er ikke komplett, men omfatter de beste og mest benyttede verktøyene. Det finnes også kommersielle verktøy i denne kategorien – for eksempel PCTel Roaming Client^a.

Verktøy	Plattform	Web-adresse	Beskrivelse
NetStumbler	Windows	www.netstumbler.com	Verktøy for søking etter aksesspunkter, måler signalstyrke og har en rekke anvendelser utover å finne ubeskyttede basestasjoner: Justering av antenne, finne forstyrrende nettverk, avsløre uregistrerte aksesspunkter, døde soner etc. Kan kombineres med GPS-data for kartlegging.
Kismet	Linux ^b	www.kismetwireless.net	Passiv monitor for trådløs nettverkstrafikk, registrerer SSID, MAC-adresser, kanaler, hastigheter og mer. Kan kombineres med GPS-data for kartlegging.
Ethereal	Unix, Mac OS X, Linux	www.ethereal.com	Trafikkanalysator med brukergrensesnitt for studie av innsamlende data i vilkårlig detalj (en 'sniffer') med intelligent pakke-deteksjon og statistikker.
AirSnort	Windows, Linux	airsnort.shmoo.com	Samler og analyserer WEP-krypterte pakker og finner til slutt krypteringsnøkkelen.
AirSnarf	Linux	airsnarf.shmoo.com	Konverterer maskinen til et aksesspunkt og demonstrerer hvordan en angriper kan bruke dette til å samle passord og annen info. Se Web for tilleggsverktøy til hjelp i forsvaret mot slike.
HostAP	Linux	hostap.epitest.fi	Konverterer maskinen til et aksesspunkt, støtte for mange 802.11i-funksjoner inklusive WPA.
WEPCrack	Unix, Linux	sourceforge.net/projects/wepcrack	Samler og analyserer WEP-krypterte pakker og finner til slutt krypteringsnøkkelen.
SMAC	Windows	www.klccconsulting.net/smac	Gjør det mulig å forandre MAC-adressen på et hvilket som helst nettverkskort under Windows (også kort som er sperret for slike forandringer fra leverandørens side).
IRPAS	Linux	www.phenoelit.de/irpas	<i>Internet Routing Protocol Attack Suite</i> – navnet forteller det meste. Programmet utnytter kjente svakheter i Internettets ruting-protokoller og i Ciscos rutere. De fleste svakheterne har vært kjent i lang tid, men er fortsatt tilstrekkelig utbredt til å gi verktøyet dramatisk effekt i mange, kanskje de fleste nettverk. En ypperlig test av robustheten i eget nett.
Ettercap	Linux, Unix	ettercap.sourceforge.net	Et mangslungent verktøy for sniffing og analyse av nettverkstrafikk, med tilleggsfunksjoner for å utføre 'man in the middle'-angrep.
Cain&Abel	Windows	www.oxid.it	En nettverkssniffer som finner og dekode passord i Windows-nettverk. Via ulike mekanismer knekkes de fleste former for passordkryptering. Verktøyet analyserer også ruting-protokoller.
Hotspotter	Unix, Linux	www.remote-exploit.org/codes.html	Søker etter passord i trådløs nettverkstrafikk og samler informasjon av hvordan og hvilke klienter som kobler seg opp. Når bildet er klart, introduserer den seg selv som aksesspunkt og overtar klientene, med interessante følger.

Tabell 1 Oversikt over Open Source-verktøy som benyttes i forbindelse med angrep på og beskyttelse av trådløse nettverk. Merk at mange av verktøyene har spesielle krav med hensyn til hvilke trådløse brikkesett som støttes. Listen er ikke komplett, men omfatter de beste og mest benyttede verktøyene. Det finnes også kommersielle verktøy i denne kategorien – for eksempel PCTel Roaming Client^a.

Verktøy	Plattform	Web-adresse	Beskrivelse
WEP Attack	Unix, Linux	sourceforge.net/projects/webattack	Samler og analyserer WEP-krypterte pakker og finner til slutt krypteringsnøkkelen. Har vist seg spesielt effektiv mot typiske hjemme-nettverk.
ASLEAP	Linux	asleap.sourceforge.net	Dekoder 'dårlige' passord innkapslet i LEAP (<i>Lightweight Extensible Authentication Protocol</i>) i tilknytning til 802.11i autentisering. Kan også hente ut filer og annen informasjon fra datastrømmen dersom den finner riktig passord.
THC-LeapCracker	Unix-lignende OS ^c	thc.org/	THC står for <i>The Hacker's Choice</i> , og presenterer en rekke verktøy i denne kategorien. Leap-Cracker har omtrent samme mål og funksjon som ASLEAP ovenfor.
THC-RUT	Unix-lignende OS	thc.org/rut	RUT (uttales <i>roof</i>) søker etter aksesspunkter med lite trafikk som er lette å angripe. Benytter flere angrepsmekanismer etter tur, og representerer første trinn i et dypere WLAN-angrep (aksess til nettverket).
Dsniff	Linux, Unix	naughty.monkey.org/~dugsong/dsniff	En samling verktøy som sniffer trafikk fra nettverket (trådløst eller tradisjonelt) og setter sammen filer, brukernavn, passord, epost-meldinger og mye annet som passerer. Også sikre protokoller som SSH og HTTPS angripes og viser seg ofte å kunne knekkes uten stor innsats.
IKEcrack	Linux	ikecrack.sourceforge.net	<i>Preshared Key (PSK) Internet Key Exchange (IKE)</i> autentisering benyttes i forbindelse med IPSec. Dette verktøyet bruker <i>brute force</i> for å knekke denne autentiseringen, og lykkes dersom nøkkelen er å finne i en ordbok (<i>dictionary attack</i>) eller har en kombinasjon av tegn som ikke er altfor hinsides enhver gjetting. En glimrende test av den reelle sikkerheten i en IPSec-forbindelse.
Nessus	Server: Linux, Unix, klient: De fleste plattformmer	www.nessus.org	Nettverksskanner av ypperste klasse – se Mellvik-Rapporten nr. 75, 77 og 86.

a 30-dagers evalueringlisens er tilgjengelig via www.pctel.com.

b De fleste verktøyene som går på Linux går også på Unix – og motsatt. Mac OS X hører under Unix i den sammenheng.

c Også under Cygwin på Windows og PalmOS – med flere.

Konklusjon

Den evige sannhet om at kunnskap er makt blir aldri mer tydelig enn når vi finner ut hva andre har visst lenge – om oss selv eller en situasjon vi har ansvaret for. Risikoen – når vi for alvor setter tennene i en slik utfordring, og oppdager hva andre har mulighet for å finne ut – er at vi oversikrer. Slik oversikring kan være bedre enn det motsatte, men representerer likevel bortkastede ressurser. Sikringstiltakene og ressursene som allokeres, må stå i forhold til de reelle truslene og verdiene som skal sikres. Så lenge vi holder denne målsetningen øverst på prioriteringslisten, er vi på rett vei.

Spennende lesestoff

Spennende, lærerikt og underholdende er nærliggende karakteristikkene av boken "*Stealing the network: How to own the box*" av Ryan Russel.

Det vi ikke vet har vi alltid vondt av – dersom andre vet. Disse og lignende verktøy er vårt beste forsvar og en nødvendig kontroll av hvordan vi ligger an i forhold til en verden der altfor mange har altfor lett tilgang til ressurser og ikke minst tid. ■