

# Gratis surfen over

Veel commerciële wifi-netwerken lek als een mandje

Tegenwoordig verschijnen steeds meer 'hotspots' – gebieden met draadloze toegang tot internet. Bij de meeste hotspots moet worden betaald en totdat betaalde, geautoriseerde toegang is verkregen, zou internetverkeer daar niet mogelijk moeten zijn. De werkelijkheid is vaak anders.

Wanneer een computer uitgerust met een wifi-kaart wordt opgestart, zal de wifi-kaart een verbinding aangaan met de hotspot. Via een protocol genaamd dhcp krijgt de computer een ip-adres. Wanneer de gebruiker nu een browser start en naar een willekeurige url gaat, zorgt speciale software ervoor dat in plaats van de opgevraagde url een login-scherm van de hotspot wordt getoond. Daar kan dan worden ingelogd, of worden betaald met een creditkaart.

Computers op internet communiceren door pakketten te sturen naar adressen van andere computers. Een voorbeeld van zo'n adres is 192.168.1.1. Dit soort adressen is niet bepaald gebruiksvriendelijk; daarom is er het 'domain name system' of kortweg dns.

Met behulp van dns kunnen gebruiksvriendelijke ip-adressen gekoppeld worden aan een veel makkelijker te gebruiken naam, ook wel 'hostnaam'. Bij het gebruik van dns worden steeds vragen gesteld, zoals bijvoorbeeld naar het ip-adres van een hostnaam.

De antwoorden op die vragen worden gegeven in de vorm van zogenaamde 'resource records' (rr's). Bij de vraag kan al worden aangegeven in wat voor rr's de vrager geïnteresseerd is. Voorbeelden van rr-types zijn:

A-records (adres), MX-records (mail exchange), Cname-records (canonical name; de gevraagde naam hierin is een alias van een andere naam) en txt-records (tekst).

Wanneer de gebruiker contact heeft met een hotspot, wordt meteen het ip-adres meegegeven van een dns-server. En nu komt het interessante: deze dns-server kan al worden gebruikt vóóordat men heeft betaald. De reden daarvoor is dat dns-functionaliteit noodzakelijk is om de gebruikelijke manier van inloggen op de hotspot te ondersteunen.

## Tunnels

Bij legitieme dns-vragen kunnen we willekeurige informatie meesturen. Door de gedistribueerde werking van het dns-systeem kunnen we ervoor zorgen dat deze informatie aankomt op een door ons gecontroleerde dns-server op internet. Bovendien kan deze dns-server weer willekeurige informatie met de antwoorden terugsturen. De heen- en weer gestuurde informatie kan naar believen worden ingevuld: er kunnen dus zelfs complete ip-pakketten in de vragen en antwoorden worden meegestuurd. We noemen dit soort constructies een 'tunnel'.

Een niet-geautoriseerde gebruiker van een hotspot kan dus een tunnel opzetten via het

dns-protocol. Hierdoor kan hij gratis gebruikmaken van de hotspot. Uiteraard is hiervoor wel speciale software nodig. Wij gebruiken een gemodificeerde variant van Nstx (<http://freshmeat.net/projects/nstx/>). Een waarschuwing is hier overigens wel op zijn plaats: Nstx heeft standaard geen enkele vorm van authenticatie. Het gebruik van Nstx is dan ook een veiligheidsrisico: immers, in principe kan iedereen een tunnel creëren naar de Nstx-server op internet. Op die manier heeft iemand rechtstreeks toegang tot deze server, zonder dat tussenliggende firewalls daar iets aan kunnen doen.

Nstx gebruikt vreemde domeinnamen om 'heengaand' verkeer te tunnelen. Terugkomend verkeer wordt 'verstopt' in txt-records. Txt-vragen zijn daarvoor uitermate geschikt omdat het antwoord vrije tekst kan bevatten. Het principe werkt als volgt. De dns-client stelt als vraag: "is er txt-informatie voor 'wat\_is\_de\_kleur\_van\_gras.example.com'." De dns-server van de hotspot speelt dit antwoord uiteindelijk door naar de Nstx-server op internet. Deze geeft als antwoord: "het

**Deze dns-server kan al worden gebruikt vóóordat men heeft betaald**

