A.J.G. Degen *

De draadloze ondergang

Draadloze netwerken zijn meer dan een rage. Ze bieden netwerktoegang onafhankelijk van kabelaansluitingen, wat bijvoorbeeld zorgt voor flexibiliteit qua werkplekken. Bedrijven kunnen zodoende heel wat besparen op de aanlegkosten voor hun intranet en interne verhuiskosten. Maar hoe zit het met de beveiliging? Kan iedereen buiten meelezen wat er binnen het bedrijf aan bedrijfsgevoelige e-mail verstuurd wordt?

Er zijn verschillende protocolstandaarden die gebruikt kunnen worden voor draadloze netwerken (in het Engels: *wireless LAN of WLAN*), zoals Bluetooth, HomeRF, IrDA (infrarood) en IEEE 802.11a en 11b. Vooral deze laatste standaard heeft de afgelopen jaren een enorme terreinwinst geboekt. De combinatie van een hoge doorvoersnelheid en een groot dekkingsgebied heeft ervoor gezorgd dat het IEEE 802.11 protocol veel wordt gebruikt, in tegenstelling tot de andere protocolstandaarden. Vandaar dat dit artikel de beveiligingsaspecten van IEEE 802.11 zal behandelen.

Management-summary

Voor een luttel bedrag is het interne computernetwerk uit te rusten met een draadloze uitbreiding. Dat het gehele interne netwerk daarmee veelal opengelegd wordt voor geïnteresseerden buiten het hek wordt over het hoofd gezien. Tenzij voldoende waarborgen zijn getroffen, is dit een goedkope manier om de organisatie ten onder te laten gaan.

De internationale standaardisatiecommissie IEEE gaf op 26 juni 1997 goedkeuring voor de 802.11 basisstandaard, de eerste internationaal erkende standaard voor draadloze netwerken. Deze standaard beschreef een draadloos netwerk met een bandbreedte van 2 Mbit/s. In een poging om deze doorvoersnelheid te verhogen, startte de IEEE verschillende werkgroepen om diverse implementaties van de IEEE 802.11 standaard te onderzoeken. (zie tabel 1)
Een uitgebreid overzicht van de werkgroepen is te vinden op de website van IEEE [1]). Het overzicht wordt deels weergegeven in tabel 1. Tot de belangrijkste werkgroepen behoren de groepen a en b, die de IEEE 802.11a en IEEE 802.11b standaarden hebben opgesteld. Beide standaarden zullen nader worden toegelicht, beginnend met de meest toegepaste versie, de IEEE 802.11b.

Verhogen

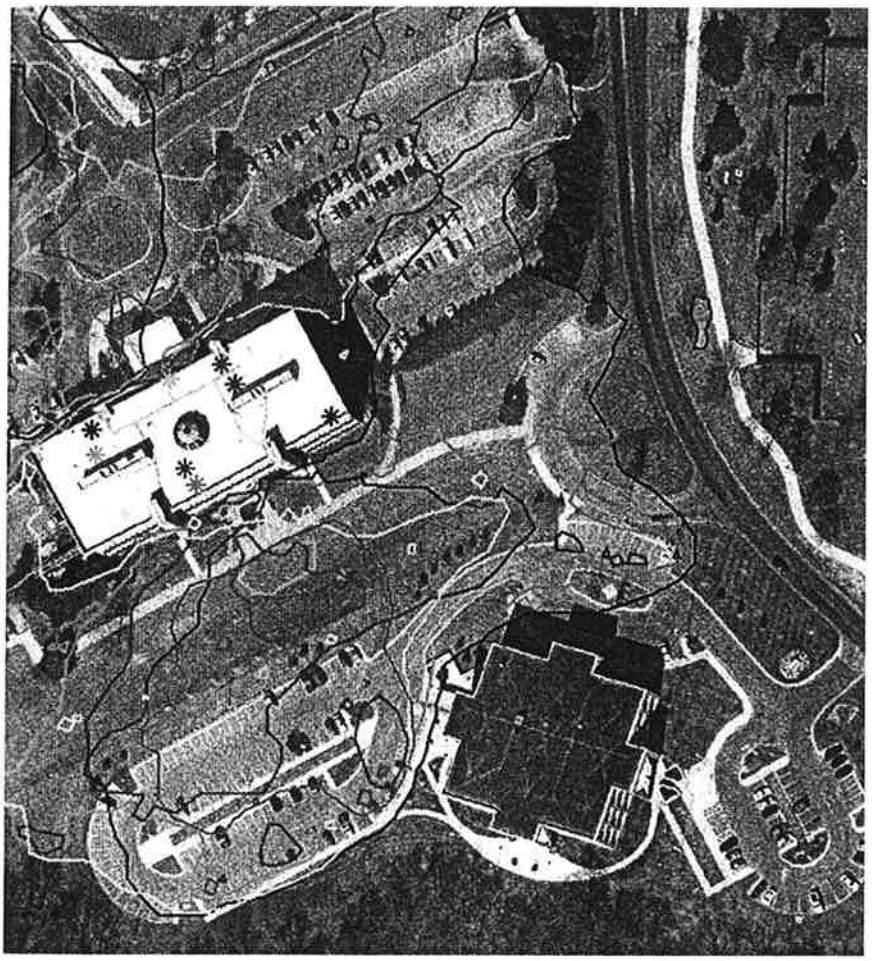
De IEEE 802.11b standaard, die in september 1999 is gepubliceerd, wist de bandbreedte te verhogen van 2 naar 11Mbit/s door een andere transmissiemethode toe te passen. Deze standaard laat echter ruimte over voor producentspecifieke implementaties. Zo wordt roaming (het automatisch overschakelen van het ene *access point* naar een ander) alleen in grove lijnen beschreven. Om ervoor te zorgen dat WLAN-apparatuur, onafhankelijk van de producent, toch onderling kan samenwerken, hebben verschillende producenten een keurmerk opgericht. Dit keurmerk is bekend onder de naam Wi-Fi.

Problemen

Werkgroep a onderzocht het gebruik van de 5 GHz band, in een poging om de doorvoersnelheid te

* werkzaam als specialist informatiebeveiliging bij TNO-FEL te Den Haag

van een bedrijf



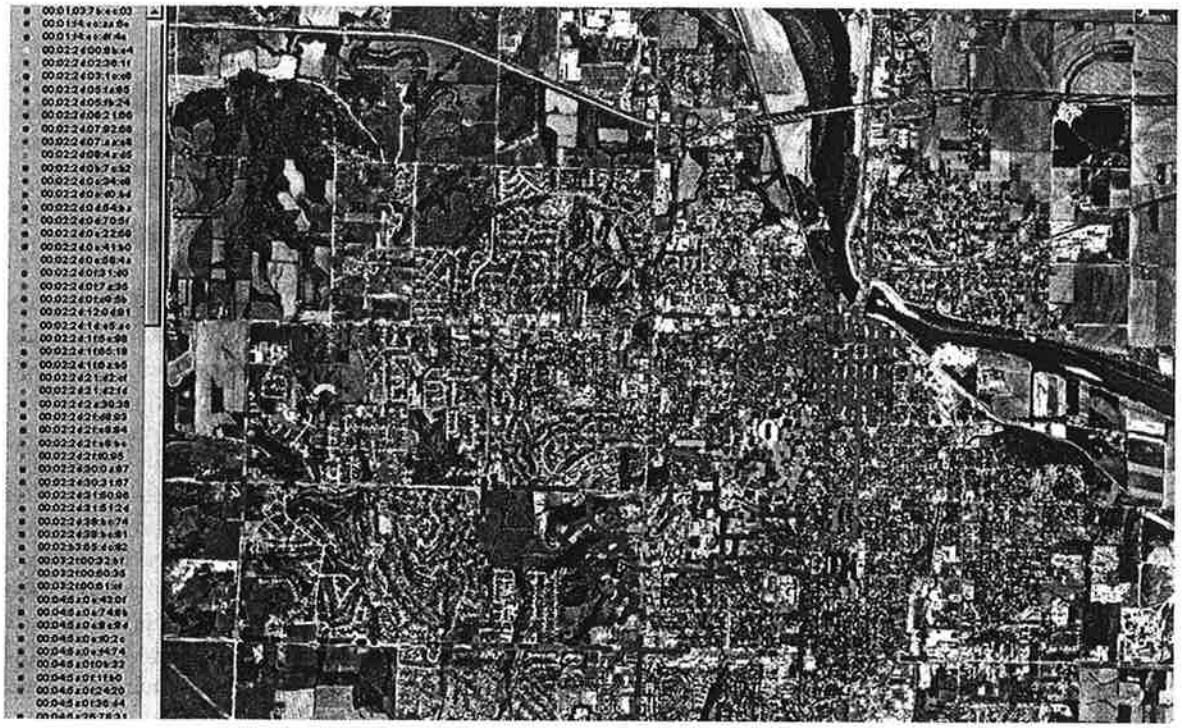
verhogen naar 54 Mbit/s. Mede door de hogere doorvoersnelheid heeft de IEEE 802.11a standaard de IEEE 802.11b standaard inmiddels opgevolgd. Een drietal problemen hebben er echter voor gezorgd dat de invoering van IEEE 802.11a apparatuur nog niet bijzonder succesvol is. Ten eerste is er een aanzienlijk aantal geavanceerde zenders en ontvangers nodig om voldoende dekking te krijgen, waardoor de kostprijs hoog is. Ten tweede moet de IEEE 802.11a standaard concurreren met de 802.11b standaard welke reeds enkele jaren voorsprong heeft. Tot slot opereert de IEEE 802.11a apparatuur in de 5 GHz band, welke in de Verenigde Staten wel vrijgegeven is, maar in Europa en Japan niet. In Europa bepaalt ieder land afzonderlijk wat er met de 5 GHz band gebeurt. Een aantal Europese landen (België, Denemarken, Finland, Frankrijk, Griekenland, Ierland, Noorwegen, Oostenrijk en Portugal) hebben al toestemming gegeven voor het vrij gebruik van op de IEEE 802.11a standaard gebaseerde producten, Nederland echter nog niet.
In Nederland wordt de 5 GHz band namelijk gebruikt door radarapparatuur en is het overige gebruik van deze band alleen toegestaan voor apparatuur die automatisch een vrije frequentie kan kiezen. Dat zorgt namelijk voor minder storing en overlast voor de radarapparatuur. Omdat de IEEE 802.11a standaard deze functie niet ondersteunt, is het gebruik ervan in Nederland nog niet goedgekeurd.
In de rest van dit artikel zullen de beveiligingsaspecten van de groep IEEE 802.11 standaarden worden besproken. Wanneer deze betrekking hebben op één van de bovengenoemde subgroepen, zal dat specifiek vermeld worden.

Niet begrensd

Tijdens het specificeren van draadloze netwerken (WLAN) gebaseerd op het 802.11 protocol is rekening gehouden met het feit dat de gegevensstroom niet begrensd is tot vooraf gespecificeerde paden. Om te zorgen dat niet iedereen het dataverkeer af kan luisteren is daarom het Wired Equivalent Privacy (WEP)

Tabel 1: overzicht belangrijkste IEEE-standaardisatiegroepen

802.11a	-	Higher frequency for communication
802.11b	-	Higher throughput in the 2.4G band by different modulation
802.11e	-	MAC Enhancement (QoS)
802.11f	-	Inter Access Point Protocol
802.11g	-	Higher Rate for IEEE Std 802.11b-1999
802.11h	-	Spectrum & Power Management Extensions for IEEE Std 802.11a-1999 in Europe
802.11i	-	Enhancements to the current 802.11 MAC to provide improvements in security



protocol ontwikkeld. Er zit echter een aantal zwakheden in dit protocol waardoor WEP geen adequate beveiligingsmaatregel is. Veel van de problemen van WEP hebben te maken met de gegenereerde sleutels die worden gebruikt om de verzonden informatie tijdens transport te versleutelen.
De cryptografische sleutel die WEP gebruikt bestaat uit twee delen: de instelbare WEP-sleutel, die na de installatie vaak niet meer wordt veranderd, en de Initialisatie Vector (IV). Deze Initialisatie Vector hoort per verstuurd pakketje te veranderen zodat de sleutel steeds varieert. Dat zou weer moeten resulteren in een betere beveiliging. Hierin zit een aantal zwakheden, waarover reeds veel in detail gepubliceerd is (zie de literatuurlijst). Enkele voorbeelden van deze zwakheden zijn: Doordat de Initialisatie Vector te klein qua lengte is, worden veel sleutels vaker hergebruikt. Dit maakt het ontcijferen een stuk eenvoudiger. Deze Initialisatie Vector hoeft volgens de WEP-standaard niet eens te veranderen. Er zijn grote groepen van zwakke sleutels die makkelijker gekraakt kunnen worden. De integriteitscontrole van ontvangen pakketten gebeurt door middel van een CRC-controle. Dit werkt goed tegen transmissiefouten, maar is niet bedoeld om zorgvuldig samengestelde frauduleuze pakketten te herkennen.

Structurele fouten

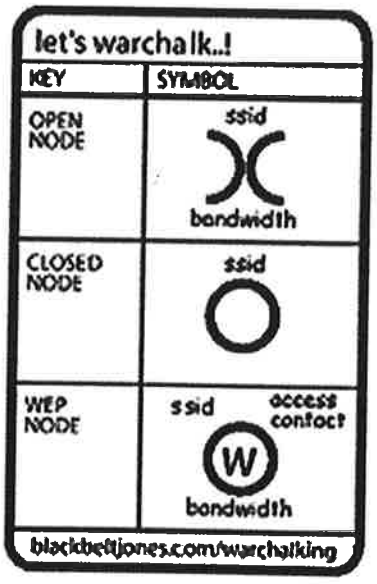
Er zijn verschillende acties ondernomen om het WEP-protocol te verbeteren. Een aantal fabrikanten heeft de WEP-implementatie uitgebreid met automatische sleuteldistributie en -management (bijv. Cisco met LEAP - Light Extensible Authentication Protocol). Dit kan echter de structurele fouten in WEP niet ongedaan maken.
Daarom is de IEEE 802.11I subgroep opgericht met het doel om de IEEE 802.11 beveiliging te verbeteren. Deze 'Robust Security Network' uitbreiding zou de beveiliging van draadloze netwerken op een hoger niveau moeten brengen. Helaas zal de standaard waarschijnlijk pas in 2004 gereed zijn.

Om de grote veiligheidsproblemen toch op korte termijn het hoofd te kunnen bieden, is er het Wi-Fi Protected Access (WPA) protocol ontwikkeld. Dit is een aangepaste versie van WEP die vanaf begin 2003 in Wi-Fi-producten toegepast zal worden. WPA maakt gebruik van Temporal Key Integrity Protocol (TKIP), dat een nieuwe sleutel gebruikt na elke 10 kilobyte aan verzonden data. Een voordeel van WPA is dat het in de huidige Wi-Fi-apparatuur gebruikt kan worden. Er zijn alleen firmware- en software-updates nodig.

Wardriving

Voor hackers en andere kwaadwillenden zijn er verschillende manieren om de zwakheden van WLANs in kaart te brengen en uit te buiten. Een van de meest gebruikte methodes om informatie over WLAN's te vergaren is 'wardriving'.
Wardriving is te vergelijken met het zoeken naar niet afgesloten elektronische deuren van een organisatie. Hierbij worden zogenaamde *access points* in kaart gebracht die ge-

bruikt kunnen worden om op het interne netwerk te komen. *Access points* zijn de kastjes waarin aan de ene kant een zender/ontvanger zit voor communicatie met de draadloos aangesloten PC's en laptops, en aan de andere kant het bedrijfsnetwerk.
Met een laptop met speciale software en een standaard draadloze LAN-kaart (IEEE 811.a of .b) kunnen *access points* in kaart worden gebracht. Wanneer dit gebeurt met een auto kunnen bijvoorbeeld de access points van hele bedrijventerreinen of een stadsdeel in een mum van tijd in kaart gebracht worden. Dit is waar de term 'wardriving' vandaan komt. Er zijn zelfs gevallen bekend van 'warflying' waarbij het in kaart brengen van de *access points* vanuit een (zweef)vliegtuig plaatsvindt [2]).
Een voorbeeld van de informatie die hierbij van de *access points* kan worden verkregen is of de WEP-encryptie al dan niet gebruikt wordt, wat de naam is van het draadloze netwerk, welke frequentie er gebruikt wordt en wie de fabrikant is van het *access point*.
Door hiernaast ook nog het verkeer af te luisteren kunnen de internet-



Figuur 1

adressen van gateways worden bepaald. Dit biedt over het algemeen voldoende informatie voor kwaadwillenden om op het WLAN in te 'breken'.
Normaal heeft een IEEE 811 *access point* een gegarandeerd bereik van vijftig meter in een kantooromgeving en tot honderd meter in de open lucht. Bij een juiste projectie lijkt het dat de communicatie binnen het hek gehouden kan worden. Niets is minder waar. We hebben het hier over gegarandeerd bereik. Signalen planten zich veel verder voort. *Wardriving* maakt hier gebruik van, al zou dat nog effectiever gaan als een *access point* vanaf grotere afstanden gedetecteerd kan worden. Hackers zetten daartoe vaak richtantennes in die het bereik gemakkelijk vergroten tot meer dan vijfhonderd meter. Daarmee is een groot gebied in korte termijn elektronisch 'af te leggen'.
Een wardriver die in enkele uren een rondje Amsterdam deed kon in principe probleemloos met zijn laptop bij bedrijven en organisaties in het bedrijfsnetwerk komen [3]).
Sommige wardrivers gebruiken het Global Positioning System (GPS) om tegelijkertijd de bedrijven en de locaties waar de beste communicatie met deze bedrijven mogelijk is in kaart te brengen. Op internet zijn overigens verschillende van dergelijke wardrive-routes gedocumenteerd.

Krijtmarkering

Om duidelijk aan te kunnen geven dat er een vrij toegankelijk draadloos netwerk in de buurt is, brengen hackers met krijt een markering aan op een muur of stoep, het zogenaamde warchalking.
Warchalking is oorspronkelijk ontstaan als een zijtak van wardriving. De symbolen die daarbij gebruikt worden lijken een standaard op zich te zijn (zie figuur 1). De resultaten van de wardriving worden direct zichtbaar gemaakt voor anderen.

Figuur 2

Er zijn twee mogelijke scenario's wanneer ergens door middel van warchalking een netwerk wordt aangegeven: Iemand heeft een netwerk gevonden en heeft de gegevens hiervan door middel van krijtmarkering beschikbaar gesteld. Het is hierbij mogelijk dat het niet de bedoeling van de eigenaar was om zijn netwerk voor anderen open te stellen. Of er is iemand die zijn draadloze netwerk expliciet beschikbaar wil stellen voor buitenstaanders.
Voor deze laatste groep heeft de Wi-Fi-alliantie een vervangende dienst opgericht, met de naam Wi-Fi Zone. Hier kan iedereen zichzelf bij aanmelden om onderdeel uit te maken van het 'Public Access program'. Alle Wi-Fi Zone geregistreerde draadloze netwerken zijn publiekelijk toegankelijk. Om onderdeel van de Wi-Fi Zone uit te maken moet het netwerk wel aan bepaalde eisen voldoen, daarnaast zijn er (in de toekomst) abonnementskosten aan verbonden. Op de site www.wi-fizone.org is een overzicht te vinden van geregistreerde zones. Dit overzicht is echter op het moment van het schrijven van dit artikel nog in ontwikkeling.
Om aan te geven dat er een Wi-Fi Zone netwerk in de buurt is, heeft de Wi-Fi alliantie ook een logo ontworpen (zie figuur 2). Het is zeer waarschijnlijk dat dit logo in de toekomst te vinden zal zijn op alle

grote vliegvelden en bij fastfoodketens. Wanneer Wi-Fi Zone aanslaat zal dit in de toekomst het fenomeen warchalking mogelijk terugdringen.

Verbeterd

Zoals eerder aangegeven is WPA een verbeterde versie van WEP. WPA bevat echter nog steeds een aantal van de structurele fouten in WEP. Doordat dit wordt opgevangen met een hoge frequentie van automatische sleutelverversing biedt het echter voldoende bescherming voor thuisnetwerken (indien daar geen gevoelige bedrijfsinformatie over gaat). Wanneer het echt belangrijk is dat bedrijfsinformatie niet kan worden afgeluisterd, zullen aanvullende beveiligingsmaatregelen getroffen dienen te worden. Hierbij zal of moeten worden gewacht op de in ontwikkeling zijnde IEEE 802.11I standaard, of het gebruik van Virtual Private Networks (VPN) boven op de WPA-beschermde draadloze verbinding. Het gebruik van VPNs versleutelt de communicatie over de draadloze verbinding op een wijze die onafhankelijk is van WEP.
Naast het versleutelen van de gegevens is er nog een andere mogelijkheid die ervoor zorgt dat een WLAN niet afgeluisterd kan worden, namelijk het afschermen van de radiosignalen. Vaak kan de zendsterkte van een *access point* worden ingesteld. Het meeste zendvermogen biedt misschien wel de grootste dekking binnen het gebouw, maar geeft daarmee ook meer mogelijkheden voor onbevoegden buiten het gebouw. Door minder zendvermogen te gebruiken wordt het bereik van het dataverkeer beperkt tot de contouren van het gebouw of het bedrijfsterrein. Toch kan dan met speciale apparatuur, zoals gevoelige richtantennes, nog steeds informatie worden ingewonnen. Om dat te voorkomen kan bijvoorbeeld aan een kooi van Faraday worden gedacht, een geaarde metalen frame dat al het radioverkeer blokkeert.
Wanneer bezoekers overigens beschikken over een palmcomputer met een draadloze LAN-adapter en automatische scan-programmatuur hebben ze nog steeds aangrijpingsmogelijkheden op uw netwerk. Het blijft een kwestie van informatieveiligheid afwegen tegen de mate van beheersinspanning en functionaliteit.

Zoals de geschiedenis ons heeft geleerd zal een gebrekkige beveiliging de groei van de markt voor draadloze netwerken niet stoppen. Veel gebruikers, waaronder telewerkers en afdelingen die onafhankelijk van de centrale ICT-voorzieningen opereren, zullen niet de moeite nemen om ingewikkelde beveiligingssoftware te installeren als hun draadloze netwerk eenmaal werkt. Zeker niet nu een setje draadloze netwerkapparatuur voor een luttel bedrag aan te schaffen is.
Daarom is het belangrijk dat er een goede, 'kant en klare' oplossing komt. Dit lijkt, met WPA en IEEE 802.11i, eindelijk in het verschiet te liggen. ■

Do's en Don'ts voor het gebruik van draadloze netwerken

Gebruik WEP met een automatisch sleutelvernieuwingsprotocol (of WPA).
Plaats *access points* zodanig dat er zo min mogelijk signaal gestraald wordt naar de openbare weg en de rijroutes en parkeerplaatsen voor bezoekers (inclusief laden en lossen).
Stel het vermogen van een *access point* niet onnodig hoog in.
Verander de netwerknaam onmiddellijk na installatie en vóór de koppeling aan het bedrijfsnetwerk.
Gebruik in geen geval de standaardwaarde.
Koppel het draadloze netwerk niet rechtstreeks aan uw bedrijfsnetwerk, maar doe dit altijd via een zorgvuldig ingestelde en beheerde firewall.
Maak de intervaltijd tussen zogenaamde *beacon broadcasts* zo groot mogelijk. Dit is het aan de buitenwereld kenbaar maken van het bestaan van het *access point*.
Overweeg om VPN-software te gebruiken tegen het afluisteren door onbevoegden.

Noten:

[1]) Overzicht van de 802.11 groepen: http://grouper.ieee.org/groups/802/11/QuickGuide_IEEE_802_WG_and_Activities.htm

[2]) Warflying http://slashdot.org/articles/02/08/18/1239233.shtml?tid=172

[3]) Amsterdam wardriving http://www.hubhop.com/home.php?refer=news&type=detail&id=63

Literatuur:

'Unsafe at any key size', Jesse R. Walker, www.dis.org/wl/pdf/unsafe.pdf

'Your 802.11 Wireless Network has No Clothes', William A. Arbaugh, Narendar Shankar, Y.C. Justin Wan, www.cs.umd.edu/~waa/wireless.pdf

'Intercepting Mobile Communications: The Insecurity of 802.11', N. Borisov, I. Goldberg, and D. Wagner, www.isaac.cs.berkeley.edu/isaac/wepfaq.html

'Weaknesses in the Key Scheduling Algorithm of RC4', Scott Fluhrer, Itsik Mantin, Adi Shamir, www.crypto.com/papers/./others/rc4_ksaproc.ps