GOVCERT.NL

FACTSHEET FS-2008-01

Draadloze netwerken

De introductie van draadloze netwerken betekende jaren geleden een doorbraak in de connectiviteit en mobiliteit van netwerkgebruikers. Door de grote flexibiliteit kunnen draadloze netwerken voor zowel thuisgebruikers als bedrijven een uitkomst zijn. Natuurlijk zijn er ook risico's aan verbonden, maar goede maatregelen verzekeren zorgeloos gebruik.

Dit factsheet beschrijft de belangrijkste standaarden, technieken en beveiligingsaspecten van Wi-Fi, de techniek die op dit moment dominant is voor draadloze netwerken. Andere technieken als Bluetooth, WiMAX, en infrarood vallen buiten de reikwijdte van dit factsheet en worden niet behandeld.[1]

Samenvatting

- Wi-Fi: gebaseerd op IEEE-standaard 802.11.
- 802.11g is momenteel dominant in de markt.
- 802.11n heeft draft-status en is nog geen standaard. Er zijn wel produkten op de markt.
- 802.11g kent een theoretische overdrachtsnelheid van 54Mbps. In de praktijk is hiervan de helft beschikbaar.
- Beschikbaarheid van draadloze verbindingen is niet te garanderen.
- Voor vertrouwelijkheid en integriteit: gebruik WPA2 of encryptie in de applicatielaag.

Standaarden: 802.11x en Wi-Fi

Wi-Fi (kort voor *wireless fidelity*) is een merknaam die in 1999 in het leven is geroepen door de Wi-Fi Alliantie. Het is bedoeld als herkenbaar "certificaat" dat gedragen mag worden door producten die zich houden aan IEEE-standaarden uit de serie 802.11[2] en die door de alliantie op interoperabiliteit zijn getest.

Voor een draadloos netwerk worden digitale signalen geschikt gemaakt voor transport over radiogolven. Technieken op basis van 802.11 (bekend als Wi-Fi) maken gebruik van de 2,4Ghz en de 5Ghz-banden.

Apparatuur op basis van 802.11g is op dit moment dominant in de markt: het biedt de hoogste snelheid met garantie op interoperabiliteit met andere apparatuur.

De belangrijkste standaarden

	Jaar	Band	Snelheid	
802.11a	1999	5Ghz	54Mbps	verouderd
802.11b	1999	2,4Ghz	11Mbps	verouderd
802.11g	2003	2,4Ghz	54Mbps	
802.11i	2004	n.v.t.	n.v.t.	beveiliging
802.11n	2009?	2,4 en 5Ghz	200+Mbps	in concept

Al enige tijd is nu ook apparatuur op basis van 802.11n op de markt. Het voornaamste kenmerk van 802.11n is de verhoging van de overdrachtsnelheid naar een theoretisch maximum van ruim 200Mbps. Deze apparatuur is niet gebaseerd op een standaard, maar op de huidige *draft 2.0* van de aankomende 802.11n-standaard. De apparatuur wordt ook op basis van deze draft gecertificeerd door de Wi-Fi Alliantie. Er is dus geen garantie dat apparatuur op basis van de *draft 2.0* in de toekomst compatible zal zijn met apparatuur op basis van de uiteindelijke standaard.

---

[1] Zie GOVCERT.NL-whitepaper over Beveiliging van mobiele apparatuur en datadragers.

[2] Dit factsheet behandelt niet alle standaarden uit de 802.11-serie. De niet genoemde standaarden beschrijven facetten van draadloze netwerken die we buiten beschouwing laten, zoals bridge operation, quality of service en roaming.
Op http://standards.ieee.org/getieee802/802.11.html staat een overzicht van de standaarden. De drafts staan op: http://standards.ieee.org/getieee802/drafts.html.

Wilhelmina van Pruisenweg 104
2595 AN Den Haag

Postbus 84011
2508 AA Den Haag

T 070 888 7 555
E info@govcert.nl
I www.govcert.nl

Snelheid en bereik

Snelheid en bereik van een draadloos netwerk zijn afhankelijk van een groot aantal factoren. Dit maakt het moeilijk om een generiek antwoord te geven op de vraag wat de reikwijdte is van een draadloos netwerk.

Van invloed op draadloze netwerken

- objecten als bomen en muren die in de weg staan
- atmosferische omstandigheden
- interferentie van andere apparaten
- de kwaliteit van de antennes van de access points (netwerkcomponenten) én de clients (gebruikers)

Een draadloos netwerk op basis van 802.11g heeft een maximale reikwijdte van ongeveer 100 meter onder normale omstandigheden[3]. Zo'n netwerk kent een theoretische overdrachtsnelheid van 54Mbps en in de praktijk is hiervan de helft beschikbaar. De overdrachtsnelheid van een draadloos netwerk neemt overigens af naarmate de afstand tot het verbindingspunt (een access point, router of andere computer) toeneemt. Bij een afstand van 100 meter kan de snelheid zijn afgenomen tot 1Mbps. Voor een optimale snelheid wordt een afstand aangeraden van maximaal 25 meter[4].

Bedreigingen en maatregelen

Tegenover het gebruiksgemak van draadloze computernetwerken staan enkele risico's, die inherent zijn aan het gebruikte medium: de radiosignalen.

Beschikbaarheid

Een belangrijk beveiligingsaspect van draadloze netwerken is dat de beschikbaarheid ervan niet gegarandeerd kan worden. Het zwakke punt is dat data wordt verstuurd door de ether, wat derden de mogelijkheid biedt om het signaal te verstoren[5]. In sommige gevallen is hiervoor zelfs geen speciale apparatuur nodig, waardoor een bewuste aanval eenvoudig is uit te voeren.[6] Daarnaast kan ook onopzettelijke interferentie van invloed zijn op de kwaliteit van de verbinding of kan de verbinding volledig worden bezet door een gebruiker die bijvoorbeeld grote bestanden download.

✓ Gebruik draadloze netwerken niet in omgevingen waar hoge beschikbaarheid noodzakelijk is.

Integriteit en vertrouwelijkheid

In standaard draadloze netwerken worden integriteit en vertrouwelijkheid van de data niet gegarandeerd. Iedereen kan immers een onversleuteld radiosignaal opvangen, afluisteren en ook manipuleren.

Encryptie in combinatie met een authenticatie-server kan afdwingen dat alleen daartoe geautoriseerde clients kunnen verbinden. Tegelijkertijd wordt hiermee het verkeer tussen client en access point versleuteld. Dit laatste is een belangrijk punt. Wi-Fi-encryptie heeft alleen effect op het radiosignaal. Zodra het verkeer het bedrade netwerk opgaat, is dit onversleuteld. Voor een bredere borging van de integriteit en vertrouwelijkheid van het verkeer, bijvoorbeeld voor telewerken, zal dus gebruik moeten worden gemaakt van aanvullende maatregelen, zoals encryptie in de applicatielaag (bijvoorbeeld VPN's, HTTPS of IP-SEC).

---

[3] Met zeer krachtige apparatuur kunnen veel grotere afstanden worden overbrugd: tot wel enkele kilometers. Dit heeft uiteraard gevolgen voor de mogelijkheden tot afluisteren van het signaal.

[4] Een inzichtelijk overzicht van de reikwijdte en sterkte van de 802.11a/b/g is te vinden op http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_white_paper09186a00801d61a3.shtml

[5] "SANDIA REPORT SAND2006-3517 EM Threat Analysis for Wireless Systems", juni 2006, §2.2 en §2.3 http://www.prod.sandia.gov/cgi-bin/techlib/access-control.pl/2006/063517.pdf

[6] Zie beveiligingsadvies GOVCERT.NL-2004-131.

Wilhelmina van Pruisenweg 104
2595 AN Den Haag

Postbus 84011
2508 AA Den Haag

T 070 888 7 555
E info@govcert.nl
I www.govcert.nl

Versleutelen met WEP of WPA?

Er zijn twee bekende versleutelingtechnieken voor draadloze netwerken: WEP en WPA.

- WEP (Wired Equivalent Privacy) is ontworpen als onderdeel van de oorspronkelijke 802.11-specificatie uit 1999. WEP als beveiligingsmaatregel is inmiddels volledig achterhaald. Het bevat meerdere zwakheden en het breken van de encryptie is triviaal. Er zijn diverse tools in omloop waarmee het kraken van WEP kinderspel is geworden.

- WPA (Wi-Fi Protected Access) en WPA2 zijn gebaseerd op de uit 2004 stammende 802.11i-standaard. WPA werd specifiek geïntroduceerd als tijdelijke oplossing voor de onvolkomenheden uit WEP en is nu opgevolgd door de definitieve standaard WPA2. WPA wordt over het algemeen onderverdeeld in WPA-PSK (*pre-shared key)*, de thuisvariant met een vooraf ingesteld wachtwoord, en een enterprise-variant, waarbij authenticatie wordt afgehandeld door een externe authenticatieserver.

WPA2 komt in grote lijnen overeen met WPA. Het belangrijkste verschil is de toevoeging van AES als encryptie-algoritme.

✓ Gebruik WPA2 in combinatie met een authenticatie-server. Alleen geautoriseerde clients kunnen zo verbinden. Overweeg wel aanvullende maatregelen als VPN's of HTTPS om verkeer van eindpunt tot eindpunt te versleutelen. Kies thuis WPA2 met een sterk (moeilijk) wachtwoord.

Aanvullende maatregelen

In het kader van draadloze netwerken noemen we ook enkele maatregelen die weliswaar niet specifiek gerelateerd zijn aan draadloze netwerken, maar wel van wezenlijk belang zijn.

- Wijzig de standaardwachtwoorden van access-points
- Schakel uPnP uit op access-points. Met behulp van uPnP kunnen ongeautoriseerde wijzigingen worden aangebracht in de configuratie van een access-point. Schakel dit daarom uit[7].
- Neem ook de firmware van access-points en draadloze netwerkkaarten mee in de patchmanagementcyclus.
- Scheidt het draadloze netwerk van het bedrade netwerk. Het access-point (en daarmee het draadloze netwerk) moet minimaal gescheiden zijn van het bedrade netwerk door middel van een firewall.

[7] Zie beveiligingsadvies GOVCERT.NL-2008-019.

Wilhelmina van Pruisenweg 104
2595 AN Den Haag

Postbus 84011
2508 AA Den Haag

T 070 888 7 555
E info@govcert.nl
I www.govcert.nl

Betwiste maatregelen

Er worden regelmatig andere maatregelen benoemd die de risico's van draadloze netwerken zouden moeten inperken. Aan de effectiviteit van deze maatregelen valt te twijfelen, zeker in relatie tot de eerder in dit factsheet genoemde maatregelen.

- Het uitzetten van SSID-broadcast (het SSID is de naam waaraan een draadloos netwerk te herkennen is) onderdrukt maar twee van de vijf soorten frames die een SSID kunnen bevatten en is geen beveiligingsmaatregel. Wij raden dit af.
- Het is niet verstandig om in een SSID melding te maken van merk en versie van het access point. Een beschrijvend SSID kan vanuit het oogpunt van gebruikersgemak zeer veel waarde hebben, ten opzichte van de marginale beveiligingswaarde van een niet-beschrijvend SSID. Wij raden aan hierin een overwogen beslissing te nemen.
- Het spoofen van een MAC-adres is triviaal. Filteren op MAC-adres voegt dus weinig toe en brengt hoge administratieve lasten met zich mee. Wij raden dit af.
- Beperking van het radiosignaal helpt om een netwerk minder bereikbaar te maken. Het bereik van het signaal is echter moeilijk vooraf te bepalen en hangt niet alleen af van de zender, maar ook van de ontvanger. Een aanvaller met zeer krachtige apparatuur kan dus een signaal opvangen dat met normale apparatuur niet meer meetbaar is. Wij raden aan hierin een overwogen beslissing te nemen.

Aanvullende informatie

- NIST Special Publication 800-48: Wireless Network Security
  http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf
  Dit document stamt al uit 2002 en is vooral verouderd waar beveiliging (WEP) betreft. De informatie over draadloze technieken en risico's is nog zeer bruikbaar.

- IEEE wireless standards zone
  http://standards.ieee.org/wireless/
  Startpunt op de IEEE-website voor informatie over standaarden en aankomende standaarden. Zeer technisch van aard.

- Wi-Fi alliance Knowledge Centre, Security
  http://www.wi-fi.org/searchresults.php?c=11&sp=Security
  Artikelen van de Wi-Fi alliance over security in draadloze netwerken. Bevat vooral aanvullende informatie over WPA, Niet technisch van aard.

- Securing WLANs using 802.11i (draft)
  http://csrp.inl.gov/Documents/Wireless%20802.11i%20Rec%20Practice.pdf
  Een vrij recent document (februari 2007) van de Idaho National Laboratory Critical Infrastructure Protection Center. Het document is nog een draft, maar is zeer bruikbaar als aanvulling op NIST-publicatie 800-48.

Over deze factsheet

GOVCERT.NL is het Computer Emergency Response Team van en voor de Nederlandse overheid. Vragen over de inhoud van deze factsheet kunt u richten aan info@govcert.nl of telefonisch via 070-8887555.