MASTER THESIS

Radboud Universiteit Nijmegen 

Beveiliging van draadloze thuisnetwerken

Auteur:	ing. Zlatko Bajić (s0721050)
Onderwijsinstelling:	Radboud Universiteit Nijmegen
Faculteit:	Faculteit der Natuurwetenschappen, Wiskunde en Informatica (FNWI)
Opleiding:	Informatiekunde
Afdeling:	Digital Security
Afstudeerbegeleider:	dr. Peter van Rossum
Afstudeernummer:	99 IK
Datum:	8 juli 2009

Inhoudsopgave

Voorwoord

Voor u ligt het resultaat van mijn afstudeeronderzoek in de vorm van de master thesis: 'Beveiliging van draadloze thuisnetwerken'. Deze thesis is geschreven in het kader van het afronden van mijn studie Informatiekunde aan de Faculteit der Natuurwetenschappen, Wiskunde en Informatica (FNWI) aan de Radboud Universiteit in Nijmegen. In het afstudeeronderzoek is onderzocht hoe Internet Service Providers in Nederland omgaan met de beveiliging van draadloze Wi-Fi thuisnetwerken en wat de huidige toestand van beveiliging in Nederland is van deze draadloze Wi-Fi thuisnetwerken.

Om dit onderzoek te realiseren, heb ik hulp gehad van verschillende mensen, die ik hierbij allemaal wil bedanken. In het bijzonder wil ik de heer Peter van Rossum bedanken voor het begeleiden van mijn afstudeeronderzoek. Daarnaast wil ik de volgende mensen bedanken voor hun bijdrage aan mijn onderzoek: de heer Ronald Sutmuller (UPC), de heer Niels Huijbregts (XS4ALL), de heer Martijn Sonius (KPN) en de heer Sven Bergman (Online).
Ten slotte wil ik iedereen bedanken die een bijdrage heeft geleverd aan dit resultaat in de vorm van hun steun, advies en vriendschap tijdens het afstudeerproces.

Veel leesplezier toegewenst,

Zlatko Bajić

Nijmegen, juli 2009

Abstract

Steeds meer mensen hebben thuis de beschikking over een breedband internetverbinding. Daarnaast maken ook steeds meer mensen gebruik van draadloze Wi-Fi netwerken om de internetverbinding, persoonlijke bestanden, printers, etc. binnenshuis met elkaar te delen. De meeste mensen weten echter niet veel over de beveiliging van deze draadloze netwerken en de bijbehorende risico's. Uit eerdere wereldwijde onderzoeken (waaronder in Nederland) blijkt dat veel draadloze thuisnetwerken slecht zijn beveiligd. We hebben hier te maken met een aanzienlijk maatschappelijk probleem, wat snel aangepakt moet worden. Het gebruikmaken van een slecht beveiligd draadloos thuisnetwerk brengt namelijk vele risico's met zich mee. Anderen kunnen gemakkelijk op een netwerk inloggen en gebruik maken van iemands internetverbinding, om bijvoorbeeld in het ergste geval spam, kinderporno of terroristische berichten te verspreiden. Daarnaast zijn de eigen persoonlijke bestanden ook niet veilig. Bankgegevens, creditcardgegevens, e-mailberichten, etc. kunnen gemakkelijk worden onderschept. Er wordt inbreuk gedaan op de persoonlijke levenssfeer van mensen; dit wordt in onze westelijke maatschappij als een groot probleem gezien. Internet Service Providers spelen hier een belangrijke rol in, omdat zij de mensen moeten voorlichten over de beveiliging van draadloze thuisnetwerken en de bijbehorende risico's. Het is dus belangrijk om te weten hoe Internet Service Providers in Nederland omgaan met de veiligheid van draadloze thuisnetwerken, vandaar de volgende onderzoeksvraag:

> *Hoe gaan Internet Service Providers in Nederland om met de veiligheid van draadloze thuisnetwerken?*

Om deze onderzoeksvraag te kunnen beantwoorden is een War Driving onderzoek uitgevoerd, waarbij in een bepaald gebied in Nederland iets meer dan 1600 draadloze Wi-Fi thuisnetwerken zijn gescand. Daarnaast is informatie over de beveiligingsvoorlichting, de aansluitingsprocedures van draadloze routers en de toekomstplannen met betrekking tot beveiliging van een aantal ISP's verkregen, door deze een vragenlijst te sturen.

Aan de hand van de onderzochte voorlichting, aansluitingsprocedures van de draadloze modems/routers en de toekomstplannen van de ISP's kunnen we concluderen dat ISP's op dit moment redelijk goed (beter dan voorheen) omgaan met de beveiliging van draadloze thuisnetwerken. De meeste draadloze modems/routers worden standaard beveiligd geleverd, de ISP's hebben speciale websites ingericht om klanten voor te lichten over de veiligheid van draadloze netwerken, er wordt uitleg gegeven over het wijzigen van de wachtwoorden, klanten worden in sommige gevallen tijdens de aansluiting dringend geadviseerd om de standaardinstellingen te wijzigen, klanten wordt een voorlichtingsmail gestuurd, etc. ISP's hebben dus werkelijk iets gedaan aan de klantenvoorlichting naar aanleiding van de in maart 2009 door OPTA ingestelde voorlichtingsplicht.

De conclusies die getrokken kunnen worden uit de verzamelde netwerkdata, ondersteunen de conclusie dat ISP's beter omgaan met veiligheid dan voorheen. Eind 2008 concludeert de consumentenbond dat in Den Haag 19% van de draadloze thuisnetwerken geheel onbeveiligd is en dat 28% van de netwerken slechts beveiligd is met de verouderde WEP encryptietechniek. 47% van de netwerken is dus onvoldoende beveiligd. Vier maanden na de invoering van de voorlichtingsplicht is 33% van de draadloze thuisnetwerken onvoldoende beveiligd. Dit is een afname van 14% en we zouden dus kunnen concluderen dat de voorlichtingsplicht hierbij geholpen heeft en dat de ISP's nu beter omgaan met de veiligheid dan voorheen.

Uit de netwerkdata kunnen we daarnaast ook concluderen dat er een verband bestaat tussen het merk draadloze router en de gebruikte encryptie. Aangezien de meeste ISP's draadloze routers van verschillende leveranciers leveren, kunnen we indirect ook vaststellen dat er een verband bestaat tussen de ISP's en de gebruikte encryptie.

Uit de netwerkdata is daarnaast gebleken dat we niet echt van een verband tussen het merk draadloze router en de routerconfiguratie kunnen spreken. De meest gebruikte merken routers hebben vaak een standaardconfiguratie.

Inleiding

Steeds meer mensen in Nederland hebben thuis de beschikking over een breedband internetverbinding. Daarnaast maken steeds meer mensen in Nederland binnenshuis gebruik van draadloze netwerktechnologie (Wi-Fi) om een eigen thuisnetwerkje op te zetten, met als doel om de internetverbinding, persoonlijke bestanden, printers, etc. binnenshuis te delen. De meeste mensen die gebruik maken van zulke draadloze thuisnetwerken zijn zich echter niet bewust van de beveiligingsrisico's die horen bij het gebruik van draadloze netwerken. Uit eerdere wereldwijde onderzoeken blijkt dat veel draadloze thuisnetwerken slecht zijn beveiligd. We hebben hier te maken met een aanzienlijk maatschappelijk probleem, wat snel aangepakt moet worden. Het gebruikmaken van een slecht beveiligd draadloos thuisnetwerk brengt namelijk vele risico's met zich mee. Internet Service Providers spelen hier een belangrijke rol in, omdat zij de mensen moeten voorlichten over beveiliging van draadloze thuisnetwerken en de bijbehorende risico's. Het is dus van groot belang om te weten hoe Internet Service Providers in Nederland omgaan met de beveiliging van draadloze thuisnetwerken en wat de huidige toestand van beveiliging in Nederland is van deze draadloze thuisnetwerken. In deze master thesis wordt een antwoord gegeven op deze vragen.

Het onderwerp van dit onderzoek is dus de beveiliging van draadloze thuisnetwerken. In deze master thesis wordt in detail beschreven welk aspect van dit onderwerp is onderzocht (probleemstelling), waarom dit aspect is onderzocht (verantwoording), hoe dit aspect is onderzocht (methode) en wat de resultaten zijn van het onderzoek (conclusie en discussie). Daarnaast wordt ook de bijbehorende theorie beschreven (theoretisch kader).
Deze master thesis is dus opgebouwd uit een aantal gedeelten. In hoofdstuk één komt de probleemstelling aan bod; het onderwerp van dit onderzoek wordt hierin geïntroduceerd samen met de bijbehorende onderzoeksvraag. Daarna wordt in hoofdstuk twee een verantwoording gegeven voor de uitvoering van dit onderzoek. Hoofdstuk drie beslaat het theoretisch kader. De theorie behorende bij de probleemstelling wordt beschreven. In hoofdstuk vier wordt de methode behandeld; de strategie van het onderzoek wordt beschreven. In hoofdstuk vijf komen de conclusie en discussie aan bod; de onderzoeksvraag en de bijbehorende deelvragen worden beantwoord. De bijlagen komen als laatste aan bod.

Bij het tot stand komen van deze master thesis is wetenschappelijke literatuur gebruikt. Een lijst met verwijzingen naar deze literatuur is als bijlage aan deze master thesis toegevoegd. Referenties naar de wetenschappelijke literatuur worden met nummers weergegeven; bijvoorbeeld [1] refereert naar het artikel, boek of onderzoeksrapport dat onder nummer één staat bij de lijst met referenties. In hoofdstuk drie (theoretisch kader) worden deze verwijzingen pas aan het einde van elke paragraaf of subparagraaf gegeven om de theorie als geheel overzichtelijk te houden.

1 Probleemstelling

Steeds meer mensen in Nederland hebben thuis de beschikking over een breedband internetverbinding [1]. Daarnaast maken steeds meer mensen in Nederland binnenshuis gebruik van draadloze netwerktechnologie (Wi-Fi) om een eigen thuisnetwerkje op te zetten, met als doel om de internetverbinding, persoonlijke bestanden, printers, etc. binnenshuis te delen [8]. De meeste mensen die gebruik maken van zulke draadloze thuisnetwerken zijn zich echter niet bewust van de beveiligingsrisico's die horen bij het gebruik van draadloze netwerken. Uit eerder onderzoek is gebleken dat in Nederland eind 2008 bijna vijftig procent van de draadloze thuisnetwerken onvoldoende beveiligd is [3]. Dit is een wereldwijd probleem; in andere landen hebben we ook te maken met hoge percentages van slecht beveiligde thuisnetwerken. In Londen (52%) [4], Parijs (25%) [6], Thessaloniki (92%) [17] en New York (39%) [5] hebben ze ook te maken met dit beveiligingsprobleem.

We hebben hier te maken met een aanzienlijk maatschappelijk probleem, wat snel aangepakt moet worden. Het gebruikmaken van een slecht beveiligd draadloos thuisnetwerk brengt namelijk vele risico's met zich mee. Anderen kunnen gemakkelijk op een netwerk inloggen en gebruik maken van iemands internetverbinding, om bijvoorbeeld in het ergste geval spam, kinderporno of terroristische berichten te verspreiden. Daarnaast zijn de eigen persoonlijke bestanden ook niet veilig. Bankgegevens, creditcardgegevens, e-mailberichten, etc. kunnen gemakkelijk worden onderschept [16]. Er wordt inbreuk gedaan op de persoonlijke levenssfeer van mensen; dit wordt in onze westelijke maatschappij als een groot probleem gezien.

Uit eerder onderzoek is daarnaast ook gebleken dat de Internet Service Providers (ISP's) in Nederland over het algemeen slecht beveiligde draadloze routers leveren aan consumenten [3]. Het is in Nederland voor ISP's namelijk niet verplicht om kant-en-klaar beveiligde Wi-Fi routers te leveren aan consumenten. Sinds kort hebben ze echter wel de verplichting om hun klanten beter voor te lichten over de beveiliging en beveiligingsrisico's met betrekking tot het gebruik van draadloze thuisnetwerken [13]. Het is dus te verwachten dat de invoering van deze voorlichtingsplicht een positief effect heeft op de beveiliging van draadloze thuisnetwerken in Nederland.

Uit de bovenstaande feiten kunnen we tot de volgende onderzoeksvraag komen:

1.1 Onderzoeksvraag

Hoe gaan Internet Service Providers in Nederland om met de veiligheid van draadloze thuisnetwerken?

2 Verantwoording

In dit onderdeel van de master thesis wordt de relevantie van dit onderzoek aangetoond. Er wordt aangetoond dat de probleemstelling nog niet bevredigend is beantwoord (nieuwswaarde), de moeite van het beantwoorden waard is (nut) en een optimale opbrengst heeft (optimalisatie).

2.1 Nieuwswaarde

Er is de afgelopen jaren wereldwijd al veel onderzoek gedaan naar de beveiliging van draadloze (Wi-Fi) computernetwerken; zowel bedrijfsnetwerken als particuliere thuisnetwerken. Hieronder wordt een samenvatting en een bespreking gegeven van de relevante onderzoeken. Daarnaast wordt ook aangegeven wat de nieuwswaarde van dit onderzoek is.

2.1.1 Eerdere onderzoeken

Een onderzoek uit Hong Kong [15], met als primaire doel de bewustmaking van de bevolking met betrekking tot beveiliging van draadloze netwerken, toont aan dat in 2002 in Hong Kong ongeveer tachtig procent van de draadloze netwerken totaal onbeveiligd is (helemaal geen encryptie). Hierbij wordt echter geen onderscheid gemaakt in bedrijfsnetwerken en thuisnetwerken. Eind 2003 is dit aantal teruggelopen naar ongeveer zeventig procent. Eind 2004 blijft de trend zich voortzetten; het aantal onbeveiligde draadloze netwerken is dan teruggelopen naar ongeveer zestig procent. Ze maken in dit onderzoek echter ook geen onderscheid in de gebruikte encryptietechnieken. Als daar ook naar was gekeken, dan zouden de cijfers veel negatiever zijn uitgepakt, aangezien sommige encryptietechnieken totaal onveilig zijn en dus gemakkelijk gekraakt kunnen worden. Ze concluderen ook dat veel netwerken nog gebruik maken van de standaard fabrieksinstellingen voor de naamgeving van het netwerk; dit kan impliceren dat de gebruikers andere standaard fabrieksinstellingen, zoals het administratief wachtwoord, ook niet hebben gewijzigd. Het merkwaardige is echter dat elk jaar het aantal draadloze netwerken in Hong Kong met meer dan twee keer groeit, terwijl het aantal beveiligde draadloze netwerken maar met ongeveer tien procent groeit per jaar. In 2002 werden ongeveer tweehonderd draadloze netwerken op een bepaalde route gedetecteerd; in 2004 was dit aantal al opgelopen tot ongeveer duizend draadloze netwerken.
Een onderzoek uit Canada [18] toont aan dat in Toronto in 2007 ongeveer vijftig procent van de draadloze netwerken onbeveiligd is en ongeveer twintig procent nog gebruik maakt van de standaard open fabrieksinstellingen. Hierbij is alleen gekeken naar draadloze netwerken in woonwijken en niet naar draadloze bedrijfsnetwerken. In dit onderzoek wordt echter ook geen onderscheid gemaakt in encryptietechnieken, waardoor de cijfers hier waarschijnlijk ook veel negatiever zouden zijn uitgevallen. In dit onderzoek hebben ze ook gekeken naar de houding van mensen tegenover het gebruik van draadloze thuisnetwerken; de meeste mensen zien er geen kwaad in om zonder toestemming gebruik te maken

van andermans draadloos thuisnetwerk. Ze rechtvaardigen dit gedrag door het gebruik te classificeren als onschadelijk en onschuldig.
Een gelijksoortig onderzoek uit New York [5] toont aan dat daar in 2008 ongeveer drie procent van de draadloze thuisnetwerken geheel onbeveiligd is; ongeveer veertig procent is slecht beveiligd (verouderde encryptietechnieken). Het aantal draadloze netwerken (thuisnetwerken en bedrijfsnetwerken) is met ongeveer vijfenveertig procent gestegen vergeleken met 2007. Ze hebben ook kunnen concluderen dat thuisnetwerken in New York vaker worden uitgerust met veilige encryptietechnieken dan bedrijfsnetwerken. Dit is uiterst merkwaardig, want je zou kunnen verwachten dat bedrijven veel beter omgaan met netwerkbeveiliging dan particulieren, wat hier duidelijk niet het geval is.
Een ander onderzoek uit de Verenigde Staten [9] toont aan dat eind 2006 ongeveer twintig procent van de internetgebruikers in de Verenigde Staten thuis een draadloos netwerk heeft.
Er is in Europa ook onderzoek gedaan naar draadloze netwerken en de beveiliging van deze netwerken. Een onderzoek van de Europese Commissie uit 2008 [8] laat zien dat ongeveer vijftig procent van de huishoudens in de Europese Unie met een internetaansluiting gebruik maakt van een draadloos thuisnetwerk. Als we alleen kijken naar huishoudens in Nederland, dan kunnen we dezelfde conclusie trekken; ongeveer vijftig procent van de huishoudens met een internetaansluiting heeft een draadloos thuisnetwerk.
In een Grieks onderzoek uit 2008 [17] wordt geconcludeerd dat in Thessaloniki (een grote Griekse stad) ongeveer vijftig procent van de draadloze netwerken geen encryptie heeft. Ongeveer veertig procent maakt alleen gebruik van een verouderde encryptietechniek. Dit betekent dat alleen ongeveer tien procent van de netwerken goed beveiligd is. Dit is een zeer verontrustende conclusie. Zij concluderen ook dat veel netwerken nog steeds gebruik maken van de standaard fabrieksinstellingen voor netwerknaamgeving; dit betekent dat de meeste mensen een draadloze router aansluiten zonder iets aan de standaard instellingen te wijzigen. In dit onderzoek wordt ook aangetoond dat het gebruik maken van MAC (Media Access Control) adresfiltering niet veilig is, omdat MAC adressen gemakkelijk gekloond kunnen worden. In dit onderzoek is echter ook geen onderscheid gemaakt in thuisnetwerken en bedrijfsnetwerken.
In andere Europese landen hebben we ook te maken met hoge percentages van slecht beveiligde thuisnetwerken. Een onderzoek uit 2008 in Londen [4] toont aan dat daar ongeveer tien procent van de draadloze thuisnetwerken onbeveiligd is. Ongeveer veertig procent van de draadloze thuisnetwerken is slecht beveiligd (verouderde encryptietechnieken). Het aantal draadloze netwerken (thuisnetwerken en bedrijfsnetwerken) is daar ook erg gegroeid (ongeveer met zeventig procent) vergeleken met 2007. In Londen is het percentage goed beveiligde draadloze thuisnetwerken ongeveer even groot als het percentage goed beveiligde draadloze bedrijfsnetwerken.
In Parijs is ook een gelijksoortig onderzoek uitgevoerd in 2008 [6]. Slechts twee procent van de draadloze thuisnetwerken is onbeveiligd. Ongeveer vijfentwintig procent is slecht beveiligd (verouderde encryptietechnieken). Het aantal

draadloze netwerken (thuisnetwerken en bedrijfsnetwerken) is in Parijs drastisch gegroeid ten aanzien van 2007; met ongeveer 550 procent. Daarnaast wordt ook geconcludeerd dat het percentage goed beveiligde draadloze thuisnetwerken in Parijs, net zo als in New York, hoger ligt dan het percentage goed beveiligde draadloze bedrijfsnetwerken, wat uiterst merkwaardig is.
In Nederland is een gelijksoortig onderzoek (op wetenschappelijk niveau) slechts één keer uitgevoerd [3]. Eind 2008 concludeert de consumentenbond dat in Den Haag ongeveer twintig procent van de draadloze thuisnetwerken geheel onbeveiligd is en dat ongeveer dertig procent van de netwerken slechts beveiligd is met de verouderde WEP encryptietechniek, die gemakkelijk te kraken is. Slechts vijftig procent van de draadloze thuisnetwerken in Nederland is dus goed beveiligd; dit is een verontrustende conclusie. Een ander onderzoek [1] toont aan dat de breedbandmarkt in Nederland in 2008 met ongeveer zes procent is gegroeid; eind 2008 zijn er bijna zes miljoen breedbandconnecties. Er wordt verwacht dat in 2009 de grens van zes miljoen wordt bereikt. Dit betekent dat in Nederland steeds meer mensen de beschikking hebben over een snelle internetverbinding, wat impliceert dat steeds meer mensen ook de mogelijkheid hebben om gebruik te maken van een draadloos netwerk, want draadloze netwerken zijn bedoeld voor snelle internetverbindingen. Een eerder genoemd onderzoek uit de Verenigde Staten [9] toont namelijk ook aan dat tachtig procent van de gebruikers van draadloze netwerken een breedband internetverbinding heeft.

2.1.2 Behoefte aan nieuw onderzoek

Uit de bovengenoemde onderzoeken kunnen we concluderen dat er wereldwijd steeds meer gebruik wordt gemaakt van draadloze thuisnetwerken en dat het over het algemeen slecht gesteld is met de beveiliging van deze netwerken. De meeste van de bovengenoemde onderzoeken kijken echter naar beveiliging van draadloze netwerken als een alleenstaande factor. Er wordt nauwelijks gekeken naar wat van invloed kan zijn op de beveiliging van de draadloze netwerken. Waarom beveiligen mensen hun draadloze netwerken niet? Zijn ze zich niet bewust van de beveiliging? Weten ze niet hoe het moet? Als je naar dit soort vragen gaat kijken, dan krijg je automatisch te maken met de Internet Service Providers (ISP's) die de draadloze routers leveren aan de consumenten, wanneer deze een internet abonnement afsluiten bij zo een provider. Een groot deel van de draadloze routers die door consumenten in Nederland gebruikt worden, zijn namelijk door de ISP's verstrekt [13]. In andere landen wordt helemaal niet gekeken naar de invloed van Internet Service Providers (ISP's) op de beveiliging van draadloze thuisnetwerken. In Nederland heeft de Consumentenbond eind 2008 wel de beveiliging van de door ISP's geleverde routers onderzocht [3], maar heeft verder niet expliciet gekeken of er verbanden bestaan tussen de gebruikte draadloze routers en de gebruikte beveiliging. Ze concluderen dat de meeste providers in Nederland onveilige draadloze routers leveren aan de consumenten. Aan de hand van dit onderzoek heeft de Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA), een onafhankelijke instantie die in

Nederland toeziet op de naleving van de wet- en regelgeving op het gebied van telecommunicatie, begin maart 2009 besloten om een voorlichtingsplicht in te stellen voor ISP's [13]. Dit houdt in dat de ISP's hun klanten beter moeten voorlichten over de beveiliging van hun draadloze thuisnetwerken (zowel bestaande klanten als nieuwe klanten). Het heeft dus nieuwswaarde om te kijken hoe de ISP's in Nederland omgaan met deze voorlichtingsplicht; hoe de aansluitingsprocedures van de draadloze routers er nu uitzien en wat de ISP's in de toekomst van plan zijn met betrekking tot de beveiliging van draadloze thuisnetwerken. Daarnaast heeft het ook nieuwswaarde om te kijken hoe de beveiligingssituatie in Nederland een aantal maanden na de voorlichtingsplicht eruit ziet en of deze is verbeterd na invoering van de voorlichtingsplicht.

2.2 Nut

We hebben hier duidelijk te maken met een maatschappelijk probleem; dit onderzoek heeft dus een maatschappelijke bijdrage. Hieronder wordt duidelijk aangegeven met welk maatschappelijk probleem we te maken hebben, wat de gewenste situatie is en wanneer we menen dat het probleem opgelost is en dus de gewenste maatschappelijke situatie is bereikt.

2.2.1 Maatschappelijk probleem

Slecht beveiligde draadloze thuisnetwerken zijn een maatschappelijk probleem. Bij iemand die een slecht beveiligd draadloos thuisnetwerk heeft, kan er misbruik worden gemaakt van de internetverbinding, persoonlijke gegevens kunnen worden achterhaald en er kan inbreuk worden gemaakt op de persoonlijke levenssfeer van diegene. We hebben daarnaast te maken met spam dat verstuurd wordt via zo een onbeveiligd draadloos netwerk, verspreiding van kinderporno, verspreiding van terroristische berichten, verspreiding van virussen, etc. We schetsen even een voorbeeld. Een nette familie in een rustig dorpje in Nederland heeft een slecht beveiligd draadloos thuisnetwerk om de internetverbinding binnenshuis te delen. Een pedofiel breekt in op het netwerk en verspreidt kinderporno op het internet via de internetverbinding van de familie. De politie komt erachter dat er kinderporno wordt verspreid via de internetverbinding van de familie. De nette vader van de familie wordt dan verdacht van verspreiding van kinderporno. Uiteindelijk, na lang onderzoek van de politie, wordt vastgesteld dat de kinderporno door iemand van buitenaf is verspreid. De nette vader en de hele familie hebben echter blijvende emotionele schade opgelopen door dit hele voorval. Als iemand eenmaal wordt verdacht van verspreiding van kinderporno, achtervolgt dit voorval diegene zijn/haar hele leven. Daarnaast heeft de politie heel veel tijd en middelen gebruikt voor het onderzoek, zonder de echte dader te hebben gevonden. Dit kost de maatschappij (belastingbetalers) natuurlijk veel geld. Uit dit weliswaar extreem voorbeeld, is het duidelijk dat we hier met een aanzienlijk maatschappelijk probleem te maken hebben.

2.2.2 Gewenste situatie

Zoals eerder aangegeven, is in Nederland dit probleem erg groot; ongeveer vijftig procent van de draadloze thuisnetwerken is slecht beveiligd. In theorie zou de gewenste situatie zijn dat er geen slecht beveiligde thuisnetwerken zijn in Nederland; in de praktijk is dit echter een onmogelijke doelstelling. We zouden tevreden zijn als minder dan tien procent van de draadloze thuisnetwerken in Nederland slecht beveiligd is.

2.2.3 Nodige kennis

Om de hierboven beschreven gewenste situatie te bereiken, is bepaalde kennis nodig. We hebben eerder aangegeven dat de meeste draadloze routers in Nederland door de Internet Service Providers zijn verstrekt aan de consumenten en dat deze routers over het algemeen onveilig zijn. De ISP's spelen dus een grote rol in deze maatschappelijke kwestie. Om iets aan dit probleem te kunnen doen, is het dus noodzakelijk om te weten hoe ISP's in Nederland omgaan met de veiligheid van draadloze thuisnetwerken. Gaan ze hier na de eerder genoemde voorlichtingsplicht anders mee om? Heeft de voorlichtingsplicht bijgedragen aan de verbetering van de beveiligingssituatie in Nederland? Is er een verband tussen de gebruikte draadloze routers en het beveiligingsniveau van de draadloze netwerken? Aan de hand van deze informatie kunnen we ook indirect vaststellen of er een verband bestaat tussen de ISP's en het niveau van beveiliging van draadloze thuisnetwerken. Om deze informatie te kunnen vergaren, is onderzoek nodig.

2.3 Optimalisatie

Hieronder wordt uitgelegd waarom de probleemstelling van dit onderzoek een optimale opbrengst en dus een groot informatiegehalte heeft.
Er wordt een uitspraak gedaan die geldt voor heel Nederland. Er is gekeken naar meerdere Internet Service Providers die in heel Nederland hun diensten aanbieden. Daarnaast wordt er een uitspraak gedaan die geldt voor alle huishoudens in Nederland, die een draadloos thuisnetwerk hebben. Als we het hebben over hoe ISP's omgaan met de veiligheid van draadloze thuisnetwerken, dan worden hier meerdere aspecten in meegenomen, zoals wat hun toekomstplannen zijn met betrekking tot de beveiliging, de aansluitingsprocedures van de meegeleverde draadloze routers, de huidige toestand van beveiliging, etc. Aangezien er naar meerdere aspecten van veiligheid is gekeken en er een uitspraak wordt gedaan die geldt voor heel Nederland, heeft dit onderzoek een groot informatiegehalte en reikwijdte; en dus ook een optimale opbrengst.

3 Theoretisch Kader

In dit deel van de master thesis wordt de probleemstelling van dit onderzoek verankerd in het bijbehorende kennisgebied. Allereerst wordt het kennisgebied ingeperkt. Daarna wordt deze inperking toegelicht. Na de inperking worden de theorieën behorende bij het kennisgebied, één voor één beschreven. Het theoretisch model, waarin de onderzoekseenheden, variabelen en relaties aan bod komen, wordt als laatste behandeld.

3.1 Inperking van het kennisgebied

Hieronder wordt het kennisgebied van dit onderzoek stap voor stap ingeperkt (van vakgebied, naar thema's, naar concreet onderwerp). Deze inperking wordt daarna verder toegelicht.

3.1.1 Inperking

- ↓ Informatica/informatiekunde (vakgebied)
- ↓ Beveiliging (thema)
- ↓ Informatiebeveiliging (thema)
- ↓ Informatiebeveiliging van computernetwerken (thema)
- ↓ Informatiebeveiliging van draadloze Wi-Fi computernetwerken (onderwerp)
- ↓ Informatiebeveiliging van draadloze Wi-Fi computernetwerken bij particulieren (concreet onderwerp)

3.1.2 Toelichting

De vakgebieden van dit onderzoek zijn informatica en informatiekunde. We hebben te maken met beide vakgebieden, omdat in dit onderzoek zowel naar de technische kanten (encryptie) als naar de minder technische kanten (omgang met) van het thema informatiebeveiliging is gekeken. Binnen deze vakgebieden hebben we te maken met het thema beveiliging van hardware en data (informatie). We hebben ons in dit onderzoek alleen beperkt tot de informatiebeveiliging; beveiliging van hardware is in dit onderzoek verder niet aan bod gekomen. Binnen het thema informatiebeveiliging hebben we te maken met de beveiliging van datastromen binnen computernetwerken. Dit kunnen we weer verder specificeren tot de beveiliging van datastromen binnen draadloze Wi-Fi computernetwerken. In dit onderzoek hebben we ons alleen beperkt tot particuliere draadloze Wi-Fi computernetwerken; draadloze bedrijfsnetwerken zijn buiten beschouwing gelaten.

3.2 Het kennisgebied

Hieronder worden de verschillende theorieën uit het kennisgebied van dit onderzoek, één voor één behandeld. De eerste vier onderwerpen (computernetwerken, draadloze computernetwerken, beveiliging van draadloze Wi-Fi computernetwerken en de bijbehorende beveiligingsrisico's) hebben specifiek te maken met de theorie achter het thema van dit onderzoek (beveiliging van draadloze thuisnetwerken). De laatste twee onderwerpen (War Driving en statistiek) hebben meer te maken met de methode van dit onderzoek. War Driving heeft te maken met de methode van dataverzameling en statistiek heeft te maken met de methode van data-analyse. Ze zijn toegevoegd aan het theoretisch kader, omdat de meeste lezers van deze master thesis waarschijnlijk weinig weten over deze twee onderwerpen en basiskennis daarover dus vereist is om de methode (komt aan bod in het volgende hoofdstuk) van dit onderzoek te kunnen begrijpen.

De te behandelen onderwerpen zijn dus:

- Computernetwerken
- Draadloze computernetwerken
- Beveiliging van draadloze Wi-Fi computernetwerken
- Beveiligingsrisico's van draadloze Wi-Fi computernetwerken
- War Driving
- Statistiek

3.2.1 Computernetwerken

Een draadloos computernetwerk combineert twee typen van communicatie technologieën; namelijk datanetwerken die het mogelijk maken om informatie (data) te delen met meerdere computers en daarnaast draadloze communicatie met behulp van elektromagnetische radiatie om informatie (data) van de ene naar de andere plek te verplaatsen. Om dus te begrijpen hoe draadloze computernetwerken werken, moet men eerst weten hoe computernetwerken in het algemeen werken. In deze paragraaf wordt globaal uitgelegd hoe computernetwerken in het algemeen in elkaar zitten.

Bits en bytes

Een computernetwerk is bedoeld om informatie (data) te verplaatsen van de ene plek naar de andere plek. Deze data heeft de vorm van bits en bytes. De processoren van computers kunnen namelijk alleen twee soorten condities herkennen; of er is wel een signaal (aangeduid met een 1) of er is geen signaal (aangeduid met een 0). Elke instantie hiervan noemen we een bit. Aan individuele bits hebben we niets. Wanneer we echter acht van deze bits aan elkaar knopen, krijgen we een byte, waarmee we 256 verschillende combinaties kunnen maken. De vorm van deze bits kan variëren; een bit kan de vorm van geluid, licht, elektrische lading of radiofrequenties aannemen. De computer krijgt de serie van bits binnen als input en produceert dezelfde serie van bits als output naar bijvoorbeeld een printer, een beeldscherm of een andere computer. Als we

het dus hebben over een computernetwerk, dan hebben we het over de bit-inputs en de bit-outputs die samen een communicatie circuit vormen. Hoe dit circuit tot stand komt (met behulp van kabels, radiogolven, licht, geluid, etc.) is eigenlijk niet van belang. Zolang we maar een communicatie circuit hebben, dan spreken we over een computernetwerk.

Protocollen

Wanneer de data (bits) zich door een computernetwerk beweegt, is het van belang dat alle betrokken actoren (verzender, ontvanger en alles daar tussenin) dezelfde regels gebruiken bij de verwerking van de data (rangschikking, timing en routering). We noemen deze set van regels een protocol. Naarmate de computernetwerken door de tijd heen steeds complexer werden, hebben de netwerkontwerpers samen besloten om het Open Systems Interconnection (OSI) model van de 'International Organization for Standardization' (ISO) als het standaardmodel voor computernetwerkcommunicatie te gebruiken. Dit model identificeert de verschillende individuele onderdelen van een netwerkconnectie. Het model is toepasbaar op bijna elke vorm van datacommunicatie systemen, dus ook voor draadloze computernetwerken. Dit model maakt het mede mogelijk dat bijvoorbeeld een complex netwerk, zoals het internet, voor een gedeelte van het signaal bekabeling gebruikt en voor een ander gedeelte van het signaal draadloze connecties. Het model wordt door bijna iedereen in de communicatie industrie gebruikt, wat ervoor zorgt dat de verschillende producten van de verschillende leveranciers met elkaar compatibel zijn.
Het OSI model bestaat uit zeven lagen. Ze worden hieronder één voor één kort behandeld. [16]

1. *Fysieke laag*: Deze laag definieert de fysieke media of hardware waarover het signaal wordt verspreid. We denken hier aan bijvoorbeeld telefoonkabels, coaxiale kabels, radiogolven, etc.
2. *Datalinklaag*: Deze laag behandelt de transmissie van data over de connectie die gedefinieerd is in de fysieke laag. Deze laag bepaalt daarnaast ook hoe de data gerangschikt (formaat) wordt.
3. *Netwerklaag*: Deze laag specificeert de route die gebruikt wordt door een signaal om zich van beginpunt naar eindpunt te verplaatsen. Het maakt hierbij niet uit of de data zich beweegt over kabels of draadloze connecties; dit wordt namelijk op een lager niveau bepaald.
4. *Transportlaag*: Op deze laag hebben we te maken met de communicatie tussen programma's op twee verschillende computers; bijvoorbeeld de connectie tussen de internet browser en de webserver van de bezochte website.
5. *Sessielaag*: Deze laag definieert het formaat dat gebruikt wordt door de applicaties uit de transportlaag om de data uit te wisselen. Het regelt dus de sessies tussen de applicaties, om bijvoorbeeld authenticatie mogelijk te maken.

6. *Presentatielaag*: Op deze laag wordt bepaald hoe de computer de ontvangen data (tekst, audio, video, etc.) behandelt; de data wordt dus gerangschikt en gestructureerd, zodat het leesbaar is voor de ontvanger.
7. *Applicatielaag*: Deze laag behandelt de opdrachten en de data die zich door het netwerk bewegen. Wanneer we bijvoorbeeld een e-mail sturen, dan zit de inhoud van deze e-mail (tekst, plaatjes, geluid, etc.) in de applicatielaag.

3.2.2 Draadloze computernetwerken

In de vorige paragraaf hebben we gekeken naar computernetwerken in het algemeen; in deze paragraaf wordt globaal uitgelegd hoe draadloze computernetwerken in elkaar zitten.

Verplaatsen van data

Het verplaatsen van data over een draadloos computernetwerk gaat gepaard met drie afzonderlijke elementen: de radiosignalen, het formaat van de data en de netwerkstructuur. Als we kijken naar het OSI (Open Systems Interconnection) model dat in de vorige paragraaf is beschreven, dan kunnen we vaststellen dat de radiosignalen bij de fysieke laag horen en dat het dataformaat in de verschillende hogere lagen zit. In de netwerkstructuur zitten de draadloze adapters en basisstations (access points/draadloze routers) die de radiosignalen verzenden en ontvangen. Deze adapters en basisstations converteren de digitale data naar radiosignalen, die ze daarna kunnen verzenden naar andere apparaten in hetzelfde netwerk. Daarnaast ontvangen ze radiosignalen van andere apparaten in het netwerk en converteren deze signalen weer terug naar digitale data, waarmee het ontvangende apparaat iets kan doen.

Voordelen en nadelen

Er zijn veel voordelen om een draadloos computernetwerk te gebruiken in plaats van een bekabeld computernetwerk. De opkomst van laptops heeft hier veel mee te maken. Laptops zijn verplaatsbare computers, dus het is veel makkelijker om gebruik te maken van een draadloos netwerk dan om steeds naar een bedrade connectie te zoeken om je laptop op aan te sluiten. Daarnaast is het mogelijk om een connectie te maken vanaf meer dan één locatie en blijft deze connectie behouden wanneer de gebruiker zich verplaatst van de ene naar de andere plek. Het is natuurlijk ook makkelijker om gebruik te maken van een draadloos signaal, dan om in je hele huis kabels aan te moeten leggen door gaten te boren in muren en kabels onder de vloeren te plaatsen, etc.
Naast de vele voordelen van draadloze computernetwerken, hebben we uiteraard ook te maken met wat nadelen; een draadloos netwerk is meestal minder veilig dan een bekabeld netwerk. Er komen veel meer beveiligingsrisico's bij kijken dan bij een bekabeld netwerk. Deze beveiligingsrisico's worden in een andere deel van dit hoofdstuk (*zie paragraaf 3.2.4 Beveiligingsrisico's van draadloze Wi-Fi computernetwerken*) behandeld.

Wi-Fi Systeem

Er zijn verschillende soorten draadloze systemen en services (Wi-Fi, WiMAX, 3G mobiele telefonie, Bluetooth, etc.) om computers en andere apparatuur, zoals mobiele telefoons, etc. te koppelen aan een lokaal netwerk of het internet; er zijn dus verschillende soorten draadloze computernetwerken. Aangezien het thema van dit onderzoek gaat over draadloze Wi-Fi thuisnetwerken, zullen wij ons hier alleen beperken tot het Wi-Fi (Wireless Fidelity) systeem. Wi-Fi staat voor draadloze lokale netwerkcommunicatie aan de hand van de IEEE (Institute of Electrical and Electronics Engineers) 802.11 standaard. De IEEE heeft een set van standaarden en specificaties (802.11) ontwikkeld voor draadloze computernetwerken die de formaten en structuur beschrijven van de korte afstandssignalen die de Wi-Fi service levert. Daarnaast zijn er extra specificaties zoals de 802.11a, 802.11b en 802.11g die wat meer zeggen over de snelheid en mogelijke radiofrequenties van de Wi-Fi service. Dit zijn de standaarden die gebruikt worden voor de meeste draadloze computernetwerken in kantoren, op publieke plekken en binnenshuis. Het Wi-Fi systeem was initieel bedoeld om een draadloze extensie te zijn van de 'Local Area Networks' (lokale bekabelde computernetwerken), waardoor de huidige standaarden alleen afstanden van maximaal 100 meter tussen ontvanger en basisstation aankunnen. Er wordt gewerkt aan een nieuwe standaard (802.11n) die grotere afstanden tussen basisstation en ontvanger ondersteunt en daarnaast ook hogere snelheden aan kan. Hieronder worden in een tabel de karakteristieken (frequentie, bereik en maximale snelheid) van de verschillende 802.11 standaarden getoond.

Tabel 1 (Karakteristieken van Wi-Fi standaarden)

Type	Radio Frequentie	Signaalbereik	Maximale snelheid
802.11b	2.4 GHz	Indoor: 30 meter Outdoor: 100 meter	11 Mbps
802.11a	5.0 GHz	Indoor: 35 meter Outdoor: 110 meter	54 Mbps
802.11g	2.4 GHz	Indoor: 35 meter Outdoor: 110 meter	54 Mbps
802.11n (voorgesteld)	2.4 GHz	Indoor: 70 meter Outdoor: 160 meter	300 Mbps

Om thuis een draadloos netwerk op te zetten op basis van het Wi-Fi systeem zijn een aantal dingen nodig:

- Een draadloze Wi-Fi router of een draadloze Wi-Fi modem en router in één.
- Een draadloze Wi-Fi netwerkkaart of een Wi-Fi USB adapter om een computer of laptop op het draadloze netwerk aan te sluiten.
- Software (drivers) voor de router/modem en netwerkkaart/USB adapter.

Andere apparaten, zoals een PDA, MP3 speler, mobiele telefoon, etc. kunnen dan ook aan het draadloze netwerk worden aangesloten, zolang ze maar het Wi-Fi systeem ondersteunen en een ingebouwde Wi-Fi ontvanger hebben. [16]

3.2.3 Beveiliging van draadloze Wi-Fi computernetwerken

In de vorige paragraaf hebben we het gehad over draadloze Wi-Fi computernetwerken; in deze paragraaf wordt de beveiliging van deze draadloze computernetwerken behandeld.

Veiligheid en encryptie

Draadloze netwerken zijn nooit geheel veilig. Het is onmogelijk om een netwerk dat gebruik maakt van radiosignalen geheel veilig te maken. Encryptie en andere beveiligingsmethodes zorgen er alleen voor dat de data moeilijker te stelen is. Het is net zoiets als het op slot doen van je auto, waardoor je auto moeilijker te stelen is, maar nooit geheel veilig zal zijn. Er is altijd een afweging nodig tussen veiligheid en gemak. Voor de meeste gebruikers komt echter het gemak van het draadloos zijn op de eerste plaats in plaats van de veiligheid.
De encryptie van data op een draadloos netwerk vindt plaats op de datalinklaag van het OSI model (*zie paragraaf 3.2.1 Computernetwerken*). Alle data die over het netwerk wordt verzonden, wordt vercijferd. Daarnaast zijn er andere encryptiemethoden zoals VPN (Virtual Private Networks) en SSL (Secure Sockets Layer) die op andere lagen opereren. Deze vallen echter buiten de scope van dit onderzoek. We concentreren ons in dit onderzoek alleen op encryptie op de datalinklaag.
De meeste nieuwe draadloze Wi-Fi modems/routers (access points) hebben ingebouwde tools om het draadloze netwerk te beveiligen met behulp van encryptie op de datalinklaag. Ze bieden meestal drie soorten encryptiemogelijkheden: WEP, WPA en WPA2. Deze worden in de paragraven hieronder één voor één behandeld.

WEP

WEP staat voor 'Wired Equivalent Privacy'. De naam zegt het al; de bedoeling was dat deze encryptiemethode een niveau van veiligheid zou bieden, die equivalent zou zijn aan de veiligheid van bekabelde computernetwerken. WEP encryptie heeft drie functies:

- Ongeautoriseerde toegang tot het netwerk tegengaan.
- Het uitvoeren van een integriteitscheck op elk datapakket.
- Het beschermen van data tegen mensen die 'afluisteren'.

WEP maakt gebruik van een geheime vercijferingssleutel om datapakketten te vercijferen voordat ze worden verzonden door een netwerkcliënt of een access point. Dezelfde sleutel wordt daarna gebruikt om de data, nadat deze ontvangen is, te ontcijferen. WEP encryptie is echter niet meer veilig. Een aantal jaren geleden is deze encryptiemethode gekraakt; een draadloos computernetwerk dat beveiligd is met WEP encryptie is totaal onveilig en is dus gemakkelijk te kraken.

WPA

WPA staat voor 'Wi-Fi Protected Access'. Deze encryptiemethode is ontwikkeld om een oplossing te bieden voor de eerdergenoemde beveiligingsproblemen van WEP. WPA is veiliger, omdat het gebruik maakt van een methode genaamd

'Temporal Key Integrity Protocol' (TKIP) om de encryptie sleutel frequent (na een bepaalde tijdsperiode of na een bepaald aantal datapakketten) te wijzigen. Dit maakt het voor een hacker moeilijker om genoeg informatie te verzamelen om de encryptie sleutel te ontcijferen. WPA is echter ook niet geheel veilig. Er zijn 'cracking' tools te vinden die de beveiliging kunnen kraken, maar deze zijn moeilijk in gebruik en het duurt meestal een lange tijd om de beveiliging te kraken. Succesvolle WPA aanvallen komen dus niet vaak voor. Zolang er een lange vercijferingssleutel met daarin willekeurige nummers wordt gekozen, is het gebruik van WPA redelijk veilig.

WPA2

WPA2 is een uitbreiding op de WPA encryptie, waarin alle verplichte elementen van de 802.11i standaard (specificatie van security mechanismen voor draadloze netwerken) zijn geïmplementeerd. WPA2 maakt gebruik van een nieuw algoritme dat als zeer veilig wordt gezien. Het wordt dus sterk aangeraden om WPA2 te gebruiken voor de beveiliging van draadloze Wi-Fi computernetwerken. [7 & 16]

3.2.4 Beveiligingsrisico's van draadloze Wi-Fi computernetwerken

In de vorige paragraaf is de beveiliging van draadloze Wi-Fi computernetwerken behandeld. In deze paragraaf wordt gekeken naar de risico's en bedreigingen van het gebruik van een draadloos Wi-Fi computernetwerk. Er wordt gekeken naar de doelstellingen van informatiebeveiliging en hoe deze doelstellingen aangevallen kunnen worden.

Doelstellingen van informatiebeveiliging

Om te kunnen bepalen wat de risico's zijn van het gebruik van een draadloos computernetwerk, moeten we eerst de doelstellingen van informatiebeveiliging behandelen. Informatiebeveiliging heeft drie hoofddoelstellingen, de zogenaamde 'CIA' doelstellingen, die hieronder één voor één beschreven worden:

- Confidentiality (confidentialiteit)
- Integrity (integriteit)
- Availability (beschikbaarheid)

Confidentiality

Aanvallen op de confidentialiteit van informatie hebben te maken met de diefstal van data of het ongeautoriseerd bekijken van data. Het doel van deze aanvallen is om toegang te krijgen tot confidentiële informatie, zoals creditcardgegevens, bankgegevens, persoonlijke gegevens, etc. Dit kan plaatsvinden door het intercepteren van data terwijl deze onderweg is of het doodgewoon stelen van datadragers. Aangezien we in dit onderzoek te maken hebben met draadloze transmissie van data, richten we ons hier alleen op het eerstgenoemde.

Integrity

Deze doelstelling heeft te maken met de betrouwbaarheid van gegevens. Aanvallen op de integriteit van informatie hebben te maken met het

ongeautoriseerd wijzigen van informatie. Dit betekent het modificeren van data terwijl deze onderweg is of wanneer deze elektronisch wordt opgeslagen. Aangezien we in dit onderzoek te maken hebben met draadloze transmissie van data, richten we ons hier ook alleen op het eerstgenoemde.

Availability
Deze doelstelling heeft te maken met het toestaan van legitieme gebruikers om toegang te hebben tot confidentiële informatie, nadat deze gebruikers zijn geauthenticeerd. De doelstelling heeft dus te maken met de beschikbaarheid van gegevens. Aanvallen op de beschikbaarheid van informatie zorgen ervoor dat de legitieme gebruikers de toegang tot de confidentiële informatie wordt geweigerd.

Aanvallen
Er zijn meerdere soorten aanvallen die uitgevoerd kunnen worden op de drie doelstellingen van informatiebeveiliging. De belangrijkste aanvallen/risico's voor draadloze computernetwerken (analyse, denial-of-service en spoofing) worden hieronder één voor één behandeld.

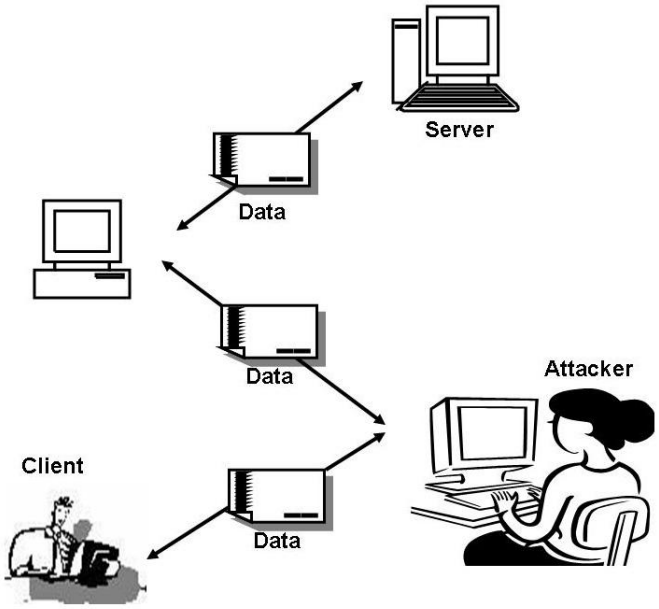
Analyse
Analyse is het bekijken, vastleggen of afluisteren van een datasignaal, dat niet bedoeld is voor degene die de analyse aan het uitvoeren is. Elk signaal dat via radiofrequenties wordt verzonden, kan afgeluisterd worden, omdat deze zich via de lucht verplaatst. Iedereen binnen het bereik van het signaal kan deze dus afluisteren. We hebben hier dus te maken met het verlies van confidentialiteit. Het is met draadloze netwerken nooit mogelijk om totale confidentialiteit te verkrijgen, omdat een signaal altijd opgevangen en vastgelegd kan worden. Dit risico is dus altijd verbonden aan het gebruik van draadloze netwerken om data te verspreiden; het kan niet worden vermeden. Het is alleen mogelijk om dit risico te verkleinen door de data te vercijferen.

Denial-of-Service
'Denial-of-Service' (DoS) is een aanval op de beschikbaarheid (availability) van informatie, zodat er niet meer gecommuniceerd kan worden binnen een computernetwerk. In draadloze netwerken worden 'DoS' aanvallen uitgevoerd door het gebruik van signaalstoorzenders. Het storen van een signaal van een draadloos netwerk is niet zo moeilijk, omdat er door de overheden bepaalde regels zijn opgesteld met betrekking tot het maximale vermogen van een draadloos netwerk. Het is dus gemakkelijk om dit lage vermogen te overtreffen door een stoorzender met een hoger vermogen te gebruiken.

Spoofing
'Spoofing' heeft te maken met het jezelf voordoen als een geautoriseerde gebruiker om toegang te verkrijgen tot een 'resource' die beveiligd is door een bepaalde vorm van authenticatie. Spoofing in draadloze computernetwerken heeft meestal te maken met het opzetten van een valse access point door de

aanvaller, met als doel om een valide gebruiker zover te krijgen om informatie over de authenticatie aan de aanvaller te verzenden. We denken hier aan bijvoorbeeld een valse hotspot in een café of iets dergelijks. Een andere manier om spoofing uit te voeren is de zogenaamde 'Man-in-the-Middle' (MiM) aanval. De aanvaller positioneert zichzelf dan tussen de gebruiker en het netwerk. Daarna gebruikt de aanvaller de authenticatie informatie, verkregen van de legitieme gebruiker, om zichzelf tegenover het netwerk voor te doen als de legitieme gebruiker. Deze aanval is hieronder afgebeeld in figuur één. [7 & 14]

Figuur 1 (Man-in-the-Middle aanval)



3.2.5 War Driving

In de vorige paragraven zijn de beveiliging en de beveiligingsrisico's met betrekking tot draadloze Wi-Fi computernetwerken behandeld. In deze paragraaf wordt een methode beschreven om draadloze Wi-Fi computernetwerken te analyseren. De methode heet War Driving. Deze methode zou ook gebruikt kunnen worden om draadloze Wi-Fi netwerken ongeautoriseerd binnen te dringen. We kijken in deze paragraaf naar de geschiedenis en achtergronden van War Driving. Daarnaast wordt ook een definitie van War Driving gegeven en er wordt gekeken naar de benodigdheden voor War Driving.

Definitie

War Driving wordt vanwege de beangstigend klinkende naam door het grote publiek en de media vaak geassocieerd met criminele activiteiten. Dit is een misvatting. War Driving is de verplaatsing door een bepaald gebied, waarbij de populatie van draadloze access points in kaart wordt gebracht voor statistische doeleinden. Deze statistische gegevens kunnen dan gebruikt worden om het bewustzijn van de beveiligingsproblemen, met betrekking tot het gebruik van draadloze computernetwerken, te verhogen. Meestal vindt War Driving plaats door, zoals de naam het al aangeeft, het rondrijden in een auto. Dit is echter niet

een criterium voor War Driving; iedereen die zich door een bepaald gebied verplaatst en data verzamelt over de aanwezige draadloze access points doet aan War Driving. Het maakt niet uit of dit nu in een auto, in een vliegtuigje, lopend, etc. plaatsvindt. Bij War Driving wordt geen gebruik gemaakt van de 'resources' van een ontdekt draadloos netwerk zonder vooraf gegeven toestemming van de eigenaar van het netwerk.

Geschiedenis en achtergronden

De term War Driving is afgeleid van de term War Dialing. War Dialing is het gebruiken van een modem, aangesloten op een computer, om een groot aantal telefoonnummers sequentieel te draaien om computers te lokaliseren die aan een modem zijn aangesloten. War Driving gebruikt in wezen hetzelfde concept, behalve dan dat het bijgewerkt is voor een meer recente technologie; namelijk draadloze computernetwerken. Het concept van het rondrijden en het in kaart brengen van draadloze netwerken begon waarschijnlijk met de utilisatie van de eerste draadloze access points. Het werd echter pas bekend toen het proces in het jaar 2000 geautomatiseerd werd door een beveiligingsexpert in de Verenigde Staten. Deze expert heeft een maandenlang onderzoek uitgevoerd naar draadloze computernetwerken in Californië en heeft zijn resultaten gepresenteerd op een beveiligingsconferentie. Deze presentatie, die als doel had om het bewustzijn van de slechte beveiliging van draadloze netwerken te verhogen, is het grondwerk van het echte War Driving.

Benodigdheden

Om War Driving uit te kunnen voeren, zijn een aantal dingen nodig. Je hebt allereerst de hardware nodig. We denken hierbij aan een laptop of een Personal Digital Assistant, oftewel een PDA. De meest gebruikelijke opzet van War Driving is die met een laptop, vandaar dat het gebruik van een PDA hier verder niet wordt behandeld. Hieronder wordt aangeven welke hardware en software nodig is wanneer War Driving met een laptop wordt uitgevoerd:

- Een laptop computer
- Een draadloze Wi-Fi netwerkkaart
- Een sterke externe antenne
- Een aansluitsnoer om de antenne aan de netwerkkaart te koppelen
- Een draagbare GPS (Global Positioning System)
- Een GPS datakabel
- Een War Driving software programma

Het kiezen van een War Driving softwareprogramma hangt vaak af van het besturingssysteem van de gebruikte laptop. Sommige programma's (zoals Kismet) werken alleen met Linux terwijl andere programma's (zoals NetStumbler en WiFi Hopper) alleen op Windows draaien.

Een typische War Driving opstelling, waarbij gebruik wordt gemaakt van een laptop, een externe antenne en een GPS ontvanger, wordt hieronder in figuur twee weergegeven. [2 & 10]

Figuur 2 (Typische War Driving opstelling met laptop, antenne en GPS)

3.2.6 Statistiek

In deze paragraaf wordt globaal gekeken naar wat statistiek is. Er wordt een definitie gegeven van statistiek, er worden een aantal basiselementen uit de statistiek behandeld en er wordt gekeken naar een aantal statistische analysetechnieken, die betrekking hebben op dit onderzoek.

Definitie

Statistiek wordt gezien als de wetenschap van gegevens (data). Deze wetenschap omvat het verzamelen, classificeren, samenvatten, organiseren, analyseren en interpreteren van numerieke informatie in de vorm van gegevens. Er zijn twee soorten gegevens; kwantitatieve en kwalitatieve gegevens. Kwantitatieve gegevens zijn meetwaarden die worden geregistreerd op een van nature voorkomende numerieke schaal, zoals temperatuur. Kwalitatieve gegevens zijn meetwaarden die niet op een natuurlijk voorkomende numerieke schaal kunnen worden geregistreerd; ze kunnen alleen worden geclassificeerd in één categorie uit een bepaalde groep categorieën.
Er zijn twee soorten statistiek; de beschrijvende statistiek en de verklarende statistiek. De beschrijvende statistiek gebruikt numerieke en grafische methoden om patronen in een gegevensverzameling te ontdekken, om de informatie die uit een gegevensverzameling kan worden gewonnen, samen te vatten en om deze informatie op een overzichtelijke manier te presenteren. De verklarende statistiek maakt gebruik van deze numerieke samenvattingen om te helpen bij het nemen van beslissingen. Er worden hierbij dus steekproefgegevens (steekproeven worden in het volgende gedeelte verder toegelicht) gebruikt voor het maken van schattingen, het nemen van beslissingen en het doen van voorspellingen of voor andere generalisaties met betrekking tot een grotere verzameling gegevens.

Basiselementen
Hieronder worden een aantal basiselementen uit de statistiek beschreven. Deze basiselementen zijn:

- Populatie
- Variabele
- Steekproef
- Statistische gevolgtrekking
- Betrouwbaarheidsmaat

Populatie
Het gebruik van statistische methoden is zeer nuttig voor het bestuderen, analyseren en kennis verkrijgen van populaties. Een populatie is een verzameling van eenheden die we willen bestuderen. Meestal zijn deze eenheden personen, objecten, transacties of gebeurtenissen. Voorbeelden van populaties van personen zijn alle kiesgerechtigden in Nederland, alle personen die een bepaald merk auto hebben of alle huishoudens in Nederland die een draadloos thuisnetwerk hebben. Voorbeelden van populaties van objecten zijn de totale voorraad onderdelen van een autofabrikant of alle mobiele telefoons van een bepaald merk. Een voorbeeld van een populatie van transacties is de totale verkoop van televisies door een elektronicawinkel in een bepaalde periode. Een voorbeeld van een populatie van gebeurtenissen is het totaal aantal dodelijke verkeersongelukken in Nederland in een bepaalde periode.

Variabele
Bij het bestuderen van een bepaalde populatie concentreren we ons op één of meer kenmerken of eigenschappen van de eenheden van die populatie. Dit noemen we de variabelen. Een variabele is dus een kenmerk of eigenschap van een individuele eenheid van een populatie. Voorbeelden van variabelen zijn leeftijd, geslacht of inkomen van alle mensen die op dit moment werkzaam zijn in Nederland. Om variabelen te kunnen bestuderen, is het nodig om een numerieke representatie voor de variabelen te vinden. Meten speelt hierbij een belangrijke rol. Meten is het proces waarbij getallen toegekend worden aan variabelen van individuele eenheden van een populatie. De leeftijd van de mensen die werkzaam zijn in Nederland meet je door ze simpelweg te vragen hoe oud ze zijn. Daarnaast zijn er natuurlijk metingen waarbij gebruik wordt gemaakt van meetinstrumenten zoals een stopwatch, liniaal, computer, etc.

Steekproef
Wanneer een te bestuderen populatie klein is, kan voor elke eenheid van die populatie een bepaalde variabele worden gemeten. We denken hierbij aan bijvoorbeeld een populatie van alle afgestudeerden aan de RU in 2008. Het resultaat is dan een telling van die populatie. Meestal zijn de populaties echter veel groter, zoals alle werknemers in Nederland of alle verkochte auto's in Nederland in 2008. Het kost dan te veel tijd en/of geld om een telling te houden voor zulke grote populaties. Een alternatief is dan om een deelverzameling van

de eenheden in een populatie te selecteren en te bestuderen. We noemen deze deelverzameling een steekproef. Je selecteert bijvoorbeeld van alle verkochte auto's in Nederland in 2008 willekeurig duizend auto's, die je dan verder gaat bestuderen.

Statistische gevolgtrekking
Nadat de variabelen voor elke eenheid in een steekproef zijn gemeten, worden de gegevens geanalyseerd. De informatie uit de steekproef kan gebruikt worden om iets te weten te komen over de hele populatie. Er worden dan statistische gevolgtrekkingen gemaakt. Een statistische gevolgtrekking is een schatting, voorspelling of een andere generalisatie met betrekking tot een populatie, gebaseerd op informatie uit een steekproef.

Betrouwbaarheidsmaat
Als er eenmaal een statistische gevolgtrekking gemaakt is op basis van informatie uit een steekproef, moet de betrouwbaarheid van deze gevolgtrekking vastgesteld worden. We moeten namelijk weten hoe goed de gevolgtrekking is. We hebben dan te maken met de betrouwbaarheidsmaat van een gevolgtrekking. Dit is een uitspraak over de mate van onzekerheid die gepaard gaat met een statistische gevolgtrekking. Meestal is deze uitspraak kwantitatief.

Statistische analysetechnieken
Er zijn een aantal technieken (gemiddelde, mediaan, standaardafwijking, groeperen, aggregeren, correlatie, tijdreeksanalyse, kruistabellen, chi-kwadraat, etc.) die gebruikt kunnen worden om de verkregen statistische gegevens te analyseren. Hieronder worden alleen de statistische analysetechnieken (kruistabellen en chi-kwadraat) behandeld die van toepassing zijn op dit onderzoek.

Kruistabellen en chi-kwadraat
Voor het analyseren van de samenhang tussen categorale variabelen wordt een kruistabel gebruikt. In een kruistabel worden de frequenties van twee variabelen tegen elkaar afgezet in één tabel. Met behulp van een kruistabel kan dus worden nagegaan of de categorieën van beide variabelen met elkaar samenhangen; dus of er sprake is van een statistisch verband. In een kruistabel kunnen de absolute celfrequenties, de verwachte celfrequenties, de relatieve celfrequenties en de residuen worden weergegeven. Aan de hand van de berekende percentages kunnen we conclusies trekken. Als de kruistabel echter gebaseerd is op steekproefgegevens geven de percentages slechts een indruk van een mogelijk statistisch verband. Met een chi-kwadraattoets kan dan worden onderzocht of er inderdaad sprake is van een statistisch verband in de hele populatie. Met deze statistische toets meet je of een statistisch verband significant is. Het standaard significantieniveau dat wordt gebruikt is 0,05. Dit betekent dat we uitgaan van een betrouwbaarheid van meer dan 95 procent om een statistisch significant verband aan te kunnen tonen. Er zijn een aantal voorwaarden bij het uitvoeren

van een chi-kwadraattoets: maximaal 20 procent van de verwachte celfrequenties mag tussen 1 en 5 liggen en het minimum aantal verwachte celfrequenties moet groter of gelijk zijn dan 1.
Om de sterkte en richting van dit verband te bepalen, wordt daarna gebruik gemaakt van associatiematen. Er zijn meerdere soorten associatiematen; welke associatiematen geschikt zijn, hangt af van de gebruikte variabelen. Als er gebruik wordt gemaakt van nominale variabelen, dan geven de associatiematen alleen informatie over de sterkte van een verband en niet over de richting. Er zijn drie associatiematen voor nominale variabelen gebaseerd op chi-kwadraat: Pearson's contingentie coëfficiënt C, Phi en Cramér's V. De Phi associatiemaat is alleen geschikt voor 2x2 (twee rijen en kolommen) tabellen; bij grotere tabellen moet de Pearson's contingentie coëfficiënt C of de Cramér's V gebruikt worden. De Pearson's contingentie coëfficiënt C wordt gebruikt als het ook van belang is hoeveel rijen en kolommen in de kruistabel zitten; als dit niet belangrijk is, kan ook Cramér's V gebruikt worden. Aan de hand van deze associatiematen kan bepaald worden hoe sterk (tussen 0 en 1) het verband is (0=geen samenhang/1=volledige samenhang). Hierbij wordt gebruik gemaakt van de hieronder getoonde vuistregels voor associatiematen. [11 & 12]

Tabel 2 (Vuistregels voor associatiematen)

Waarde associatiemaat	**Sterkte samenhang**
1	Volledige samenhang
0,75	Sterke samenhang
0,50	Matig sterke samenhang
0,25	Zwakke samenhang
0	Geen samenhang (onafhankelijkheid)

3.3 Theoretisch model

In dit gedeelte van het theoretisch kader wordt het theoretisch model beschreven. Er wordt behandeld welke domeinen en dus welke onderzoekselementen er zijn in dit onderzoek, welke variabelen aan bod komen en welke relaties verondersteld worden tussen de verschillende variabelen.

3.3.1 Domeinen en onderzoekselementen

Er zijn in dit onderzoek twee domeinen, namelijk de Internet Service Providers (ISP's) in Nederland en huishoudens in Nederland met een draadloos Wi-Fi computernetwerk. Door het uitvoeren van dit onderzoek wordt een uitspraak gedaan die geldt voor alle ISP's in Nederland en voor alle huishoudens in Nederland met een draadloos Wi-Fi thuisnetwerk. De onderzoekselementen zijn dus de ISP's en de Nederlandse huishoudens.

3.3.2 Variabelen

Er zijn vier theoretische variabelen die in dit onderzoek aan bod zijn gekomen:

- Encryptieniveau (ordinale variabele): het niveau (geen, WEP, WPA, WPA2) van encryptie van een draadloos Wi-Fi computernetwerk bij huishoudens in Nederland.
- Routerconfiguratie (nominale variabele): de instellingen (standaard, niet standaard) van de draadloze modem/router bij huishoudens in Nederland.
- Routermerk (nominale variabele): de leverancier van de draadloze modem/router bij huishoudens in Nederland.
- Beveiligingsomgang (nominale variabele): de omgang met beveiliging van draadloze thuisnetwerken door de ISP's.

De eerste drie variabelen (encryptieniveau, routerconfiguratie en routermerk) horen bij de onderzoekselementen huishoudens in Nederland die een draadloos Wi-Fi computernetwerk hebben. De variabele beveiligingsomgang heeft betrekking op de onderzoekselementen Internet Service Providers in Nederland.

3.3.3 Relaties

In dit onderzoek is getoetst of er een samenhang bestaat tussen de variabele encryptieniveau en de variabele routermerk. We hebben gekeken of het encryptieniveau afhankelijk is van het routermerk (en dus indirect ook van de ISP). Daarnaast is getoetst of er een samenhang bestaat tussen de variabele routerconfiguratie en de variabele routermerk. Er is dus ook gekeken of de routerconfiguratie afhankelijk is van het routermerk (en dus indirect ook van de ISP).

4 Methode

In dit onderdeel van de master thesis wordt beschreven wat de onderzoeksfunctie en de structuur (deelvragen) van dit onderzoek zijn. Daarnaast wordt de operationalisatie van het onderzoek behandeld (onderzoekseenheden, variabelen, indicatoren, validiteit, dataverzameling en data-analyse).

4.1 Onderzoeksfunctie

Dit onderzoek had twee soorten onderzoekselementen; namelijk Internet Service Providers (ISP's) in Nederland en huishoudens in Nederland die een draadloos Wi-Fi thuisnetwerk hebben. Aangezien we met twee soorten onderzoekselementen te maken hadden, bestond dit onderzoek ook uit twee gedeeltes en had het dus twee onderzoeksfuncties: een toetsingsgedeelte en een beschrijvingsgedeelte.

4.1.1 Toetsen

We wilden toetsen of er een samenhang bestaat tussen het encryptieniveau van draadloze Wi-Fi thuisnetwerken en het merk van de gebruikte draadloze router. Indirect konden we dan ook vaststellen of er samenhang bestaat tussen het encryptieniveau en de ISP's, omdat de ISP's verschillende merken draadloze routers leveren aan de consumenten. Daarnaast wilden we ook toetsen of er een samenhang bestaat tussen de routerconfiguratie en het merk van de gebruikte draadloze router; en dus indirect ook tussen routerconfiguratie en de ISP's.

4.1.2 Beschrijven

We wilden beschrijven hoe de ISP's in Nederland omgaan met de beveiliging van draadloze thuisnetwerken. We hebben gekeken of er grote variaties bestaan tussen de verschillende ISP's wat betreft beveiligingsomgang of dat ze allemaal ongeveer hetzelfde doen met betrekking tot dit aspect.

4.2 Onderzoeksstructuur

In deze paragraaf wordt de onderzoeksstructuur behandeld. De onderzoeksvraag wordt opgesplitst in deelvragen en er wordt beschreven hoe het antwoord op de onderzoeksvraag eruit moest komen te zien.

4.2.1 Deelvragen

De onderzoeksvraag is opgesplitst in een aantal deelvragen. Met behulp van de resultaten van deze deelvragen kon de algemene onderzoeksvraag beantwoord worden. Om er achter te komen hoe de Internet Service Providers in Nederland omgaan met de veiligheid van draadloze thuisnetwerken (onderzoeksvraag), moest het volgende worden onderzocht:

- Aansluitingsprocedures van de door ISP's geleverde draadloze routers.
- Voorlichting van consumenten door ISP's over beveiliging van draadloze thuisnetwerken.

- Toekomstplannen van de ISP's met betrekking tot de beveiliging van draadloze thuisnetwerken.
- Huidige toestand van beveiliging van draadloze thuisnetwerken in Nederland.

Aan de hand van de vier bovengenoemde punten konden de volgende deelvragen worden geformuleerd (alle deelvragen hebben alleen betrekking op Nederland)**:**

- Wat is de huidige toestand van beveiliging van draadloze thuisnetwerken?
- Is de beveiliging van draadloze thuisnetwerken verbeterd na de invoering van de voorlichtingsplicht voor Internet Service Providers?
- Is er een verband tussen het merk (leverancier) wi-fi router en het encryptieniveau van draadloze thuisnetwerken?
- Is er een verband tussen het merk (leverancier) wi-fi router en de routerconfiguratie?
- Welke merken wi-fi routers worden door de verschillende Internet Service Providers aan de consumenten geleverd?
- Wat doen de Internet Service Providers aan voorlichting met betrekking tot beveiliging van draadloze thuisnetwerken?
- Hoe ziet de aansluitingsprocedure van de geleverde wi-fi routers eruit met betrekking tot beveiliging?
- Wat zijn de Internet Service Providers van plan om in de toekomst te doen met betrekking tot beveiliging van draadloze thuisnetwerken?

4.2.2 Antwoord op de onderzoeksvraag

Het antwoord op de onderzoeksvraag moest uit twee gedeeltes bestaan. Allereerst gingen we kijken of er verbanden bestaan tussen de variabele routermerk en de variabelen encryptieniveau en routerconfiguratie. Het antwoord hierop moest er dan als volgt uitzien:

- Er bestaat wel/geen significant verband tussen routermerk (en indirect ISP) en encryptieniveau.
- Er bestaat wel/geen significant verband tussen routermerk (en indirect ISP) en routerconfiguratie.

Het andere gedeelte van het antwoord moest bestaan uit een beschrijving van hoe ISP's omgaan met de veiligheid van draadloze thuisnetwerken, waarbij moest worden gekeken naar de huidige voorlichting, de aansluitingsprocedures van de geleverde draadloze routers en de toekomstplannen van de ISP's met betrekking tot beveiliging van draadloze thuisnetwerken. Daarnaast moest ook worden behandeld of er grote verschillen bestaan tussen de verschillende ISP's, wat betreft de omgang met beveiliging van draadloze thuisnetwerken, of dat ze allemaal ongeveer op hetzelfde niveau zitten.
Aan het eind zouden de twee gedeeltes gekoppeld kunnen worden, door bijvoorbeeld te kijken of dat ISP's die slecht omgaan met de beveiliging ook slecht scoren op het gebied van encryptieniveau en routerconfiguratie.

4.3 Operationalisatie

In dit gedeelte van de methode worden het steekproefkader, de indicatoren, de interne validiteit en de externe validiteit behandeld.

4.3.1 Steekproefkader

Met dit onderzoek moest een representatieve uitspraak gedaan kunnen worden, die geldt voor alle Internet Service Providers in Nederland en voor alle huishoudens in Nederland die een draadloos thuisnetwerk hebben. We hadden hier dus te maken met twee steekproefkaders:

- Steekproef van de ISP's in Nederland.
- Steekproef van huishoudens in Nederland die een draadloos Wi-Fi thuisnetwerk hebben.

Om een representatieve uitspraak te kunnen doen, die geldt voor alle ISP's in Nederland, moest aan de volgende eisen worden voldaan:

- De te onderzoeken ISP's moeten de vijf grootste ISP's van Nederland zijn, omdat deze representatief zijn voor de Nederlandse breedbandmarkt.
- Er moeten zowel kabelinternet ISP's als ADSL-internet ISP's in het onderzoek worden meegenomen.
- De te onderzoeken ISP's moeten draadloze routers leveren aan de consumenten.
- De te onderzoeken ISP's moeten hun diensten aanbieden in grote gedeeltes van Nederland (dus geen regionale ISP's).

Aan de hand van deze eisen zijn de volgende ISP's geselecteerd:

- Kabelinternet: Ziggo en UPC
- ADSL-internet: KPN, Tele2 en XS4ALL

Om een representatieve uitspraak te kunnen doen, die geldt voor alle huishoudens in Nederland die een draadloos thuisnetwerk hebben, moest aan de volgende eisen worden voldaan:

- Er moeten minimaal duizend huishoudens onderzocht worden, omdat in eerdere onderzoeken ook ongeveer deze aantallen zijn gebruikt.
- Het onderzoek moet plaatsvinden in een gebied waar genoeg draadloze thuisnetwerken in gebruik zijn; dus geen kleine dorpen (minimaal 15000 inwoners).
- Het onderzoek moet plaatsvinden in een gebied waar meerdere ISP's (zowel kabelinternet als ADSL-internet) hun diensten aanbieden.
- Het onderzoek moet plaatsvinden in een gebied dat representatief is voor Nederland, op basis van inkomen en de demografische samenstelling van de bevolking.

Aan de hand van deze eisen zijn de volgende huishoudens geselecteerd:

- Duizend willekeurige huishoudens met een draadloos Wi-Fi thuisnetwerk in de regio Waalwijk/Drunen.

4.3.2 Indicatoren

Hieronder wordt beschreven hoe de variabelen zijn vastgesteld; dus welke indicatoren gebruikt zijn om de verschillende variabelen vast te stellen.

De variabele encryptieniveau is vastgesteld door de volgende indicator:

- Gebruikte encryptiemethode -> geen, WEP, WPA, WPA2.

De variabele routerconfiguratie is vastgesteld door de volgende indicator:

- SSID (Service Set Identifier) van het draadloze netwerk -> standaard, niet standaard (als in de SSID het merk van de router voorkomt, kunnen we aannemen dat we met een standaard routerconfiguratie te maken hebben).

De variabele routermerk is vastgesteld door de volgende indicator:

- MAC-adres van de draadloze router.

De variabele beveiligingsomgang is vastgesteld door de volgende indicatoren:

- Aansluitingsprocedures van de draadloze routers met betrekking tot beveiliging.
- Huidige klantenvoorlichting door ISP's met betrekking tot beveiliging.
- Toekomstplannen van ISP's met betrekking tot beveiliging.

4.3.3 Interne Validiteit

De interne validiteit van dit onderzoek is gewaarborgd, doordat de indicatoren om de variabelen encryptieniveau (gebruikte encryptiemethode), routerconfiguratie (SSID) en routermerk (MAC-adres) standaard indicatoren zijn om deze variabelen vast te stellen en in eerdere onderzoeken ook zijn gebruikt. De indicatoren om de beveiligingsomgang vast te stellen, zijn ook valide, omdat we hiermee alle factoren hebben behandeld die ISP's daadwerkelijk kunnen doen met betrekking tot beveiliging van draadloze thuisnetwerken. We hebben zowel de technische (aansluitingsprocedures) als de niet-technische kanten (voorlichting en toekomstplannen) van omgang met beveiliging onderzocht.

4.3.4 Externe Validiteit

De externe validiteit van dit onderzoek is gewaarborgd, doordat beide steekproefkaders zo zijn opgesteld dat ze voldoen aan de opgestelde eisen (*zie paragraaf 4.3.1 Steekproefkader*). De onderzochte ISP's bestaan zowel uit kabelinternet providers als ADSL-internet providers, ze leveren allen draadloze routers en ze bieden allen hun diensten aan in grote gedeeltes van Nederland. De onderzochte huishoudens komen uit een gebied dat representatief is voor heel Nederland, ze komen uit een gebied waar meerdere ISP's hun diensten aanbieden en ze komen uit een gebied waar genoeg draadloze thuisnetwerken in gebruik zijn.

4.4 Dataverzameling

In deze paragraaf wordt beschreven hoe de data, die nodig was voor dit onderzoek, is verzameld.
We hadden in dit onderzoek te maken met twee soorten data:

- Netwerkdata
- Data van de Internet Service Providers

De dataverzameling van beide datasoorten wordt hieronder behandeld.

4.4.1 Netwerkdata

De netwerkdata is verzameld door gebruik te maken van de methode War Driving (*zie paragraaf 3.2.5 War Driving*). Er is in de regio Waalwijk/Drunen door woonwijken rondgereden met een laptop met geïnstalleerde War Driving software, een sterke antenne en een GPS ontvanger (Nokia LD-3W). Er is gekozen om de War Driving tool WiFi Hopper 1.2.2 te gebruiken, omdat deze beschikbaar is als een volledige evaluatieversie, GPS ontvangst ondersteunt en op Windows draait.

4.4.2 Data van de Internet Service Providers

De data van de Internet Service Providers is verzameld door via e-mail contact op te nemen met de geselecteerde ISP's en ze een aantal vragen te stellen die betrekking hebben op hun omgang met de beveiliging van draadloze thuisnetwerken (*zie Bijlage 3: ISP Vragenlijst*). Er bestond natuurlijk altijd de mogelijkheid dat de geselecteerde ISP's geen informatie zouden willen verschaffen. Daarom zijn ook een aantal reserve ISP's geselecteerd: Telfort, Alice, en Online. Daarnaast was er ook de mogelijkheid (in het geval van geen respons) om op gebruikersforums naar informatie te zoeken over de aansluitingsprocedures en de gegeven voorlichting.

4.5 Data-analyse

In de vorige paragraaf is al aangegeven dat we met twee soorten data te maken hadden; namelijk de netwerkdata en de data van de ISP's. De data-analyse van beide datasoorten wordt hieronder behandeld.

4.5.1 Netwerkdata

De verzamelde netwerkdata is met behulp van statistiek geanalyseerd. Het programma dat hiervoor is gebruikt, is het statistisch analyseprogramma SPSS 16 voor Windows. De verzamelde data is ingevoerd in een kruistabel (*zie Bijlage 1: Kruistabellen*). Om te bepalen of er een verband bestaat tussen de variabelen routermerk en encryptieniveau èn routermerk en routerconfiguratie is een chi-kwadraattoets uitgevoerd, waarbij we uitgegaan zijn van het standaard significantieniveau van 0,05 (*zie paragraaf 3.2.6 Statistiek*). Als de overschrijdingskans dat chi-kwadraat wordt overschreden kleiner was dan 0,05 procent, dan zouden we te maken hebben met een statistisch significant verband tussen de variabelen.

Om daarna te meten hoe sterk het verband is tussen de variabelen, is een op chi-kwadraat gebaseerde nominale associatiemaat Pearson's contingentie coëfficiënt C gebruikt, waarbij uitgegaan is van de volgende vuistregels voor associatiematen:

Tabel 3 (Methode: Vuistregels voor associatiematen)

Waarde associatiemaat	**Sterkte samenhang**
1	Volledige samenhang
0,75	Sterke samenhang
0,50	Matig sterke samenhang
0,25	Zwakke samenhang
0	Geen samenhang (onafhankelijkheid)

Er is gekozen voor de Pearson's contingentie coëfficiënt C, omdat we met grote kruistabellen te maken hadden en het van belang was hoeveel rijen en kolommen de kruistabellen hadden.
De chi-kwadraattoets en de associatiemaat Pearson's contingentie coëfficiënt C zijn automatisch berekend door SPSS. We zouden spreken van een echt verband tussen routermerk en encryptieniveau èn tussen routermerk en routerconfiguratie als de waarden van de associatiematen hoger zouden zijn dan 0,50.

4.5.2 Data van de Internet Service Providers

De antwoorden op de gestelde vragen (*zie Bijlage 3: ISP Vragenlijst*) zijn gebruikt om per Internet Service Provider te beschrijven hoe deze omgaat met de veiligheid van draadloze thuisnetwerken. Deze omgang is bepaald door de indicatoren aansluitingsprocedure, huidige voorlichting en toekomstplannen. Per ISP zijn deze indicatoren behandeld. Uiteindelijk kon er worden gekeken of er veel variatie bestaat tussen de verschillende ISP's of dat ze ongeveer op hetzelfde niveau zitten wat betreft de beveiligingsomgang. Daarna kon deze data gekoppeld worden aan de netwerkdata, om bijvoorbeeld te kijken of ISP's die slecht omgaan met de beveiliging ook slecht scoren op het gebied van encryptieniveau en routerconfiguratie.

5 Conclusie en discussie

Dit onderzoek bestond uit twee gedeeltes, namelijk het toetsingsgedeelte en het beschrijvingsgedeelte. De conclusie en discussie bestaan dus allereerst ook uit twee gedeeltes (toetsen en beschrijven). Hierin worden de verschillende deelvragen afzonderlijk beantwoord. Daarna wordt de gehele onderzoeksvraag beantwoord en worden voorstellen gedaan voor toekomstig onderzoek.

5.1 Toetsen

De volgende deelvragen hebben betrekking op dit gedeelte van de conclusie en discussie:

- Wat is de huidige toestand van beveiliging van draadloze thuisnetwerken?
- Is de beveiliging van draadloze thuisnetwerken verbeterd na de invoering van de voorlichtingsplicht voor Internet Service Providers?
- Is er een verband tussen het merk (leverancier) wi-fi router en het encryptieniveau van draadloze thuisnetwerken?
- Is er een verband tussen het merk (leverancier) wi-fi router en de routerconfiguratie?

Om deze deelvragen te kunnen beantwoorden, zijn met behulp van War Driving (*zie hoofdstuk 4 Methode*) 1816 draadloze Wi-Fi thuisnetwerken gescand (*zie Bijlagen*). Om te kunnen voldoen aan de voorwaarden van de chi-kwadraattoets (*zie paragraaf 3.2.6 Statistiek*) zijn de merken draadloze modems/routers die niet meer dan twintig keer voorkomen, verwijderd. Uiteindelijk zijn er 1653 draadloze modems/routers overgebleven. Deze War Driving netwerkscanning voldoet aan de in de methode genoemde eisen. Er zijn genoeg netwerken gescand en het gebied waar is gescand, is representatief voor heel Nederland met betrekking tot demografische samenstelling en ISP aanbod.
De hierboven genoemde deelvragen worden hieronder één voor één beantwoord.

Wat is de huidige toestand van beveiliging van draadloze thuisnetwerken?

Er zijn 1653 draadloze thuisnetwerken gescand. 138 (8,3%) van deze netwerken hebben helemaal geen beveiliging. 407 (24,6%) netwerken zijn beveiligd met de verouderde WEP encryptie. 425 (25,7%) netwerken zijn beveiligd met WPA encryptie. 683 (41,3%) netwerken zijn beveiligd met WPA2 encryptie. Dit betekent dat 1108 (67%) van de gescande netwerken goed beveiligd zijn (WPA of WPA2). 545 (33%) van de gescande netwerken zijn slecht beveiligd (geen encryptie of de verouderde WEP encryptie).
Van de 1653 gescande netwerken heeft 1030 (62,3%) een SSID die als standaard kan worden gekenmerkt. 623 (37,7%) draadloze netwerken hebben geen standaard SSID.
De merken Thomson (26% van totaal), Cisco-Linksys (17,7%), Siemens (12,5%), Sitecom (11,1%) en Netgear (9,5%) zijn de meest voorkomende merken draadloze modems/routers.

Is de beveiliging van draadloze thuisnetwerken verbeterd na de invoering van de voorlichtingsplicht voor Internet Service Providers?

Eind 2008 concludeert de consumentenbond dat in Den Haag 19% van de draadloze thuisnetwerken geheel onbeveiligd is en dat 28% van de netwerken slechts beveiligd is met de verouderde WEP encryptietechniek. 47% van de netwerken is dus onvoldoende beveiligd.
Begin maart 2009 heeft de OPTA de voorlichtingsplicht voor ISP's ingevoerd (*zie hoofdstuk 2 Verantwoording*). Vier maanden na de invoering van deze voorlichtingsplicht is 8,3% van de netwerken geheel onbeveiligd en 24,6% slecht beveiligd (WEP). Dit betekent dat dus vier maanden na de invoering van de voorlichtingsplicht 33% van de draadloze thuisnetwerken onvoldoende beveiligd is. Dit is een afname van 14% en we zouden dus kunnen concluderen dat de voorlichtingsplicht hierbij geholpen heeft.
Er moet echter in acht worden genomen dat dit onderzoek niet in Den Haag is uitgevoerd (de consumentenbond heeft het onderzoek in Den Haag gedaan). Dat zou ook het verschil in beveiliging kunnen verklaren. Hier gaan we echter niet van uit, omdat er geen (voor dit onderzoek) wezenlijke verschillen zijn tussen Den Haag en de regio Drunen/Waalwijk.

Is er een verband tussen het merk (leverancier) wi-fi router en het encryptieniveau van draadloze thuisnetwerken?

Met behulp van de gemaakte kruistabel (*zie Bijlage 1: Kruistabellen*) is een chi-kwadraattoets uitgevoerd om te bepalen of er een verband bestaat tussen de twee variabelen (routermerk en encryptieniveau). Hieronder is de uitkomst van deze toets (uit SPSS) weergegeven.

Tabel 4 (SPSS chi-kwadraattoets - routermerk*encryptieniveau)

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	908,249[a]	39	,000
Likelihood Ratio	946,313	39	,000
N of Valid Cases	1653		

a. 9 cells (16,1%) have expected count less than 5. The minimum expected count is 1,67.

De chi-kwadraattoets is geldig, omdat aan de voorwaarde is voldaan dat maximaal 20% van de verwachte celfrequenties tussen 1 en 5 mag liggen en het minimum aantal verwachte celfrequenties groter of gelijk is dan 1*(9 cells (16,1%) have expected count less than 5. The minimum expected count is 1,67)*.
We zijn uitgegaan van het standaard significantieniveau 0,05. Als de overschrijdingskans dat chi-kwadraat wordt overschreden kleiner is dan 0,05 procent, dan hebben we te maken met een statistisch significant verband tussen de twee variabelen. De overschrijdingskans is 0,000. Er is dus een statistisch significant verband tussen de twee variabelen.

Om te meten hoe sterk het verband is, is daarna een op chi-kwadraat gebaseerde nominale associatiemaat Pearson's contingentie coëfficiënt C gebruikt. De uitkomst hiervan (uit SPSS), wordt hieronder weergegeven.

Tabel 5 (SPSS Pearson's contingentie coëfficiënt - routermerk*encryptieniveau)

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,595	,000
N of Valid Cases		1653	

We hebben eerder aangegeven (*zie hoofdstuk 4 Methode*) dat we pas spreken van een echt verband tussen routermerk en encryptieniveau als de waarde van de associatiemaat hoger is dan 0,50. In dit geval is de waarde van de associatiemaat 0,595 en kunnen we ook spreken van een echt verband (matig sterke samenhang) tussen routermerk en encryptieniveau; het encryptieniveau is dus enigszins afhankelijk van het routermerk.

Opmerkelijke cijfers

- 73,7 procent van de Thomson modems/routers zijn beveiligd met WPA2; 7,9 procent zijn beveiligd met WPA.
- 100 procent van de AVM modems/routers zijn beveiligd met WPA2.
- Slechts 8,9 procent van de Netgear modems/routers zijn beveiligd met WPA2; 82,2 procent zijn beveiligd met WPA.
- Slechts 13,7 procent van de Sitecom modems/routers zijn beveiligd met WPA2; 35,5 procent zijn beveiligd met WPA.
- 83,1 procent van de Siemens modems/routers zijn beveiligd met WPA2; slechts 0,5 procent is beveiligd met WPA.

De bovengenoemde cijfers tonen ook aan dat wel degelijk uitmaakt welke modem/router er gebruikt wordt en welke beveiliging hierbij toegepast wordt.

Is er een verband tussen het merk (leverancier) wi-fi router en de routerconfiguratie?

Met behulp van de gemaakte kruistabel (*zie Bijlage 1: Kruistabellen*) is een chi-kwadraattoets uitgevoerd om te bepalen of er een verband bestaat tussen de twee variabelen. Hieronder is de uitkomst van de toets (uit SPSS) weergegeven.

Tabel 6 (SPSS chi-kwadraattoets routermerk*routerconfiguratie)

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	436,143[a]	13	,000
Likelihood Ratio	456,878	13	,000
N of Valid Cases	1653		

a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 7,54.

De chi-kwadraattoets is geldig, omdat aan de voorwaarden is voldaan dat maximaal 20% van de verwachte celfrequenties tussen 1 en 5 mag liggen en het aantal minimum verwachte celfrequenties groter of gelijk is dan 1*(0 cells (,0%) have expected count less than 5. The minimum expected count is 7,54)*.
We zijn uitgegaan van het standaard significantieniveau 0,05. Als de overschrijdingskans dat chi-kwadraat wordt overschreden kleiner is dan 0,05 procent, dan hebben we te maken met een statistisch significant verband tussen de twee variabelen. De overschrijdingskans is 0,000. Er is dus een statistisch significant verband tussen de twee variabelen.
Om te meten hoe sterk het verband is, is daarna een op chi-kwadraat gebaseerde nominale associatiemaat Pearson's contingentie coëfficiënt C gebruikt. De uitkomst hiervan (uit SPSS), wordt hieronder weergegeven.

Tabel 7 (SPSS Pearson's contingentie coëfficiënt C - routermerk*routerconfiguratie)

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	,457	,000
N of Valid Cases		1653	

We hebben eerder aangegeven (*zie hoofdstuk 4 Methode*) dat we pas spreken van een echt verband tussen routermerk en routerconfiguratie als de waarde van de associatiemaat hoger is dan 0,50. In dit geval is de waarde van de associatiemaat 0,457 en kunnen we dus niet spreken van een echt verband tussen routermerk en routerconfiguratie. We zitten met deze waarde namelijk tussen een zwakke samenhang en een matig sterke samenhang.

Opmerkelijke cijfers

- 85,8 procent van de Thomson modems/routers heeft een SSID die standaard blijkt te zijn.
- 80,9 procent van de Netgear modems/routers heeft een SSID die standaard blijkt te zijn.
- 80,7 procent van de Siemens modems/routers heeft een SSID die standaard blijkt te zijn.
- 71,0 procent van de Sitecom modems/routers heeft een SSID die standaard blijkt te zijn.
- 75,0 procent van de AVM modems/routers heeft een SSID die standaard blijkt te zijn.
- 29,3 procent van de Cisco-Linksys modems/routers heeft een SSID die standaard blijkt te zijn.

Uit deze cijfers is af te leiden dat bij de veelvoorkomende merken modems/routers (met uitzondering van Cisco-Linksys) de SSID standaard blijkt te zijn; wat ook kan impliceren dat de gehele routerconfiguratie standaard is. Deze cijfers tonen ook aan dat er niet echt een duidelijk verband bestaat tussen routermerk en routerconfiguratie.

5.2 Beschrijven

De volgende deelvragen hebben betrekking op dit gedeelte van de conclusie en discussie:

- Welke merken wi-fi routers worden door de verschillende Internet Service Providers aan de consumenten geleverd?
- Wat doen de Internet Service Providers aan voorlichting met betrekking tot beveiliging van draadloze thuisnetwerken?
- Hoe ziet de aansluitingsprocedure van de geleverde wi-fi routers eruit met betrekking tot beveiliging?
- Wat zijn de Internet Service Providers van plan om in de toekomst te doen met betrekking tot beveiliging van draadloze thuisnetwerken?

Om deze deelvragen te kunnen beantwoorden, is contact opgenomen met de vijf geselecteerde ISP's (*zie hoofdstuk 4 Methode*). Daarnaast is voor de zekerheid meteen ook contact opgenomen met de drie reserve ISP's. Van de acht gecontacteerde ISP's hebben vier ISP's meegedaan aan het onderzoek. Dat waren KPN, UPC, XS4ALL en Online. Alice gaf aan dat ze geen draadloze router meer leveren. Telfort wilde wel bijdragen aan het onderzoek, maar ze hebben tot op de dag van vandaag geen informatie geleverd. Ziggo en Tele2 hebben helemaal geen reactie gegeven. De vier ISP's die mee hebben gedaan aan het onderzoek, voldoen allen aan de opgestelde eisen (*zie hoofdstuk 4 Methode*). De onderzochte ISP's bestaan zowel uit kabelinternet providers (UPC) als ADSL-internet providers (KPN, XS4ALL en Online), ze leveren allen draadloze modems/routers en ze bieden allen hun diensten aan in grote gedeeltes van Nederland. De externe validiteit van dit onderzoek is hiermee dus gewaarborgd. Er moet wel in acht worden genomen dat de verkregen informatie van de ISP's zelf komt. Het is dus best mogelijk dat de genoemde toekomstplannen met betrekking tot voorlichting en aansluitprocedures van de modems/routers loze beloftes zijn; deze informatie kan niet gecontroleerd worden. De huidige aansluitprocedures en de huidige voorlichting konden wel gecontroleerd worden. De hierboven genoemde deelvragen worden hieronder één voor één beantwoord. Per deelvraag worden de onderzochte ISP's één voor één behandeld.

Welke merken wi-fi routers worden door de verschillende Internet Service Providers aan de consumenten geleverd?

- KPN levert de KPN Experia Box, oftewel een Thomson TG787v (modem en router in één) van de leverancier 'Thomson Telecom Belgium'.
- UPC levert nu een Netgear RangeMax WPN824v2 (alleen router) van de leverancier 'Netgear Inc.'; vanaf 20 juli 2009 gaan ze de Netgear WNR2000 (alleen router) van de leverancier 'Netgear Inc.' en de Sitecom WL308 (alleen router) van de leverancier 'Sitecom Europe BV' leveren.
- XS4ALL levert de FRITZ!Box 7170 (modem en router in één) van de leverancier 'AVM'.
- Online levert de Thomson SpeedTouch ST706WL (modem en router in één) van de leverancier 'Thomson Telecom Belgium'.

Wat doen de Internet Service Providers aan voorlichting met betrekking tot beveiliging van draadloze thuisnetwerken?

KPN geeft haar klanten op een aantal manieren voorlichting over de beveiliging. Ten eerste worden klanten gedurende de installatie met de installatie CD-ROM dringend geadviseerd om hun draadloze netwerk te beveiligen met een WPA sleutel en om de SSID van het netwerk aan te passen. De installatie CD-ROM helpt de klant om deze procedure verder uit te voeren. Daarnaast is op de website van KPN een speciale pagina gemaakt (www.kpn.com/veilig-internetten) om klanten voor te lichten over het beveiligen van hun computer en hun draadloos netwerk. Op deze webpagina worden klanten erop geattendeerd dat ze hun draadloos netwerk met beveiliging dienen in te stellen om misbruik te voorkomen. Daarnaast zijn op deze webpagina van alle modems/routers die KPN levert (en in het verleden heeft geleverd) handleidingen beschikbaar voor het instellen van de beveiliging. In deze handleidingen wordt ook uitleg gegeven over de verschillende encryptietechnieken (WEP, WPA en WPA2), waarbij ook wordt aangegeven dat WEP gekraakt kan worden. Daarnaast worden bij de oplevering van het abonnement de klanten in een welkomst e-mail gewezen op het belang van een goede beveiliging en worden ze verwezen naar de eerder genoemde webpagina. Er wordt op deze webpagina echter nergens aandacht besteed aan de problemen die voorkwamen met eerdere Thomson routers (zoals de Thomson ST780WL) waarbij het standaard wachtwoord afgeleid kon worden uit de SSID; er bestond een wiskundige relatie tussen de sleutel en de SSID.

UPC heeft een speciale voorlichtingspagina op het internet ingericht om hun klanten voor te lichten over de beveiliging van draadloze netwerken: http://www.upc.nl/internet/veilig_internet/beveiliging_draadloze_router. Op deze webpagina wordt globaal uitgelegd hoe draadloze netwerken werken en wat de bijbehorende risico's zijn. Daarnaast wordt kort uitgelegd hoe draadloze netwerken beveiligd kunnen worden (versleuteling en MAC-adres filtering). Er wordt ook aangegeven dat de router van UPC standaard beveiligd (WPA) wordt geleverd. Ze geven op deze webpagina ook aan dat het mogelijk is om het standaard wachtwoord te wijzigen om meer zekerheid over de veiligheid van de verbinding te hebben; hierbij wordt een document geleverd, waarin wordt beschreven hoe het wachtwoord van de router die nu geleverd wordt, veranderd kan worden. Er wordt echter niet gesproken over het veranderen van de standaard SSID. In de, bij het installatiepakket bijgeleverde, UPC handleiding worden de verschillende begrippen (WEP, WPA, SSID, etc.) kort behandeld; daarnaast wordt aangegeven dat de draadloze UPC router veilig is, omdat deze standaard wordt ingesteld met WPA beveiliging. Er wordt echter nergens genoemd dat WEP een sterk verouderde (kraakbare) encryptietechniek is.

XS4ALL geeft voorlichting over de beveiliging op hun speciale veiligheidspagina: http://www.xs4all.nl/veiligheid/draadloos. Hierop worden de risico's beschreven, die horen bij het gebruiken van een draadloos netwerk. Daarnaast wordt uitleg gegeven over de beveiliging (encryptietechnieken, sleutels, etc.) van een

draadloos netwerk. Hierbij wordt duidelijk aangegeven dat WEP een verouderde methode is en dat er voor WPA/WPA2 moet worden gekozen. In de bijgeleverde handleiding wordt het onderwerp beveiliging uitvoerig behandeld. Hierin wordt duidelijk aanbevolen dat de vooraf ingestelde netwerksleutel en de SSID zo snel mogelijk gewijzigd moeten worden; de wijzigingsprocedures komen ook uitvoerig aan bod. In de handleiding wordt ook aangegeven dat WEP een verouderde techniek is en dat WEP sleutels binnen enkele uren gekraakt kunnen worden. Ze raden dus dringend aan om een Wi-Fi adapter met WPA of WPA2 te gebruiken.

Online voegt bij het installatiepakket van de modem/router een informatie flyer toe welke uitleg geeft over de aanwezige draadloze beveiliging en ook een instructie geeft hoe deze beveiliging verder verhoogd kan worden. Ze verwijzen naar informatie op hun website: www.online.nl/modemveiligheid. Op deze website wordt uitgelegd hoe de draadloze modem/router verder beveiligd kan worden (veranderen van de sleutel en het onzichtbaar maken van de netwerknaam). Er wordt ook uitleg gegeven over de encryptiemethoden WEP en WPA. Ze zetten er echter niet bij dat WEP een zeer onveilige encryptiemethode is; het enige wat ze zeggen, is dat WPA wat veiliger is dan WEP.

Hoe ziet de aansluitingsprocedure van de geleverde wi-fi routers eruit met betrekking tot beveiliging?

KPN levert in het installatiepakket van de modem/router een installatie stappenplan, een installatie CD-ROM en een installatiehandleiding. Het netwerk wordt standaard met WPA2 beveiligd. Tijdens het installeren van de modem/router met de installatie CD-ROM worden klanten dringend geadviseerd om het draadloze netwerk te beveiligen met een WPA sleutel en om de SSID van het netwerk aan te passen. De installatie CD-ROM helpt de klant om deze procedures verder uit te voeren. De nieuw ingevoerde gegevens van de klant worden door KPN op een server bewaard in het KPN netwerk. Mocht de modem/router een ‘factory reset’ nodig hebben, dan kunnen de gegevens teruggezet worden op de modem/router. Daarnaast is in de installatiehandleiding als bijlage, informatie over draadloos internetten toegevoegd. Hierin wordt onder andere verteld dat je een SSID code en een WPA sleutel nodig hebt om een draadloze connectie te kunnen maken en dat deze gegevens op de sticker op de onderkant van de modem/router te vinden zijn. Er wordt hier echter niets gezegd over het veranderen van de sleutel en het aanpassen van de SSID.

UPC levert in het installatiepakket van de router een installatie CD-ROM, een UPC installatiehandleiding en een Engelstalige routerhandleiding (standaard retailversie). De router wordt standaard geleverd met WPA beveiliging. Tijdens de installatie wordt de gebruiker gedwongen om een SSID en WPA wachtwoord te kiezen die niet gemakkelijk te raden zijn. In de UPC installatiehandleiding wordt echter niets gezegd over het wijzigen van deze gegevens. Op de website van UPC is wel een Nederlandstalige instructie te vinden over hoe het wachtwoord gewijzigd kan worden.

XS4ALL levert in het installatiepakket van de modem/router een gedrukte korte handleiding, een installatie CD-ROM en een digitale lange handleiding. Met behulp van de installatie CD-ROM kan de modem/router voorbereid worden op het gebruik. De installatiehulp op de installatie CD-ROM beschrijft de stappen die nodig zijn voor de eerste ingebruikname van de modem/router. De modem/router wordt standaard beveiligd bij de installatie. In de handleiding wordt aanbevolen om het standaard wachtwoord en SSID zo snel mogelijk te wijzigen; er wordt echter alleen voor de wijziging van het wachtwoord de procedure beschreven (wijzigen van de SSID blijft buiten beschouwing).

Online levert in het installatiepakket van de modem/router een flyer over de inhoud van het installatiepakket, een installatieposter, een installatie CD-ROM en een informatie flyer die de klanten erop attendeert dat de modemveiligheid verder verhoogd kan worden. In de installatieprocedure (stappenplan en installatie CD-ROM) komt de beveiliging niet aan bod; de modem/router wordt echter standaard geïnstalleerd met WPA encryptie met een standaard wachtwoord dat wiskundig af te leiden is uit de voor iedereen zichtbare naam van de router (SSID). In de bijgeleverde informatie flyer wordt wel gerefereerd naar de website van Online waar uitgelegd staat hoe het standaard wachtwoord gewijzigd kan worden en de SSID onzichtbaar kan worden gemaakt.

Wat zijn de Internet Service Providers van plan om in de toekomst te doen met betrekking tot beveiliging van draadloze thuisnetwerken?

KPN is van mening dat ze op dit moment al het mogelijke doen om een goede voorlichting aan consumenten te geven met betrekking tot beveiliging van draadloze thuisnetwerken. Ze zien op dit moment geen verdere verbeterpunten. Als in de toekomst blijkt dat er verbeteringen mogelijk zijn, zullen ze de informatievoorziening en/of de beveiliging up-to-date brengen.

UPC gaat vanaf 20 juli 2009 twee nieuwe draadloze routers leveren, die ook voorzien zijn van WPA2 beveiliging. Daarnaast zijn ze van plan om in samenwerking met de leveranciers aan ‘customization’ van de routers te werken en om de routers onder andere te voorzien van ‘UPC plug&play’ software. Ze zijn daarnaast ook van plan om een Nederlandstalige handleiding van de routers te leveren en om de speciale veiligheidspagina aan te vullen met betrekking tot de twee nieuwe routers (o.a. instructies om het standaard wachtwoord te wijzigen).

XS4ALL doet al veel aan veiligheid en heeft dus geen concrete veranderplannen.

Online is op dit moment bezig met een traject om een opvolger te vinden voor de huidige Thomson SpeedTouch 706WL modem/router. De nieuwe modem/router zal standaard geconfigureerd worden met WPA2 beveiliging en een WPS functionaliteit om voor een betere beveiliging en een gemakkelijkere installatie te zorgen. Daarnaast blijft Online op regelmatige basis gesprekken voeren met de leverancier van de routers betreffende het verder aanscherpen van de veiligheid.

5.3 Antwoord op de onderzoeksvraag

Dit onderzoek is uitgevoerd met als doel om op de volgende onderzoeksvraag een antwoord te kunnen geven:

- Hoe gaan Internet Service Providers in Nederland om met de veiligheid van draadloze thuisnetwerken?

Uit de antwoorden op de deelvragen, die in de vorige paragraven zijn behandeld, kunnen we concluderen dat Internet Service Providers in Nederland beter omgaan met de veiligheid van draadloze thuisnetwerken dan voorheen (de OPTA heeft niet voor niets de voorlichtingsplicht ingesteld; ISP's gingen voorheen niet echt goed om met de veiligheid van draadloze thuisnetwerken).

Aan de hand van de onderzochte voorlichting, aansluitingsprocedures van de draadloze modems/routers en de toekomstplannen van de ISP's kunnen we concluderen dat ISP's op dit moment redelijk goed omgaan met de beveiliging van draadloze thuisnetwerken. De meeste draadloze modems/routers worden standaard beveiligd geleverd, de ISP's hebben speciale websites ingericht om klanten voor te lichten over de veiligheid van draadloze netwerken, er wordt uitleg gegeven over het wijzigen van de wachtwoorden, klanten worden in sommige gevallen tijdens de aansluiting dringend geadviseerd om de standaardinstellingen te wijzigen, klanten wordt een voorlichtingsmail gestuurd, etc. ISP's hebben dus werkelijk iets gedaan aan de voorlichting naar aanleiding van de ingestelde voorlichtingsplicht. Het zou wel beter zijn om de beveiliging meer te integreren in de bijgeleverde handleidingen; het ziet er nu naar uit dat in de meeste gevallen de beveiliging achteraf is toegevoegd of in een extra informatie flyer wordt behandeld. Beveiliging moet een standaard onderdeel worden van de aansluiting en de voorlichting. Daarnaast moeten klanten er meer op geattendeerd worden dat WEP een verouderde en onveilige beveiliging is en niet meer gebruikt zou moeten worden. Er zou ook meer aandacht besteed moeten worden aan de procedures om de SSID van een netwerk te wijzigen; dit valt nu vaak buiten beschouwing.

De conclusies die getrokken kunnen worden uit de verzamelde netwerkdata, ondersteunen de conclusie dat ISP's beter omgaan met veiligheid dan voorheen. Eind 2008 concludeert de consumentenbond dat in Den Haag 19% van de draadloze thuisnetwerken geheel onbeveiligd is en dat 28% van de netwerken slechts beveiligd is met de verouderde WEP encryptietechniek. 47% van de netwerken is dus onvoldoende beveiligd. Vier maanden na de invoering van de voorlichtingsplicht is 33% van de draadloze thuisnetwerken onvoldoende beveiligd. Dit is een afname van 14% en we zouden dus kunnen concluderen dat de voorlichtingsplicht hierbij geholpen heeft en dat de ISP's nu beter omgaan met de veiligheid dan voorheen. Er kunnen echter ook andere oorzaken zijn van deze verbetering; mensen besteden bijvoorbeeld zelf meer aandacht aan de beveiliging door bijvoorbeeld berichtgeving in de media over dit onderwerp.

Uit de netwerkdata kunnen we daarnaast ook concluderen dat er een verband bestaat tussen het merk draadloze router en de gebruikte encryptie. Aangezien de meeste ISP's draadloze routers van verschillende leveranciers leveren, kunnen we indirect ook vaststellen dat er een verband bestaat tussen de ISP's en de gebruikte encryptie. Er moet wel in acht worden genomen dat dit verband wordt aangenomen en niet echt is bewezen; verder onderzoek zou zich kunnen richten om dit verband expliciet te bewijzen (*zie paragraaf 5.4 Mogelijkheden voor toekomstig onderzoek*).

Uit de netwerkdata is daarnaast gebleken dat we niet echt van een verband tussen het merk draadloze router en de routerconfiguratie kunnen spreken. De meest gebruikte merken routers hebben een standaardconfiguratie. Hierbij moet echter ook in acht worden genomen dat we aan de hand van de SSID hebben bepaald of een routerconfiguratie standaard is of niet; een standaard SSID hoeft niet altijd te betekenen dat de rest van de configuratie ook standaard is.

5.4 Mogelijkheden voor toekomstig onderzoek

In de verantwoording van dit onderzoek (*zie hoofdstuk 2 Verantwoording*) is al aangegeven dat de meeste van de onderzoeken op dit gebied alleen kijken naar beveiliging van draadloze netwerken als een alleenstaande factor. Er wordt nauwelijks gekeken naar wat van invloed kan zijn op de beveiliging van de draadloze netwerken. Waarom beveiligen mensen hun netwerken niet? Zijn ze zich niet bewust van de beveiliging? Weten ze niet hoe het moet? Als je naar dit soort vragen gaat kijken, dan krijg je automatisch te maken met de Internet Service Providers (ISP's) die de draadloze modems/routers leveren aan de consumenten, wanneer deze een internet abonnement afsluiten bij zo een internet provider.
In dit onderzoek hebben we geprobeerd om de factor die de ISP's spelen in kaart te brengen. We hebben nu slechts kunnen impliceren dat er een verband bestaat tussen de ISP's en de gebruikte encryptie. Dit zou verder onderzocht kunnen worden door in plaats van de netwerken te scannen (met War Driving) een enquête te houden, waarbij mensen daadwerkelijk worden gevraagd bij welke ISP ze zijn aangesloten en welke encryptiemethode ze gebruiken. Met de verkregen gegevens, kan duidelijk worden onderzocht of er echt een verband bestaat tussen ISP's en de gebruikte encryptiemethode.
Mogelijke toekomstige onderzoeken zouden zich ook kunnen richten op andere factoren op dit gebied. Er zou bijvoorbeeld naast een War Driving onderzoek in een bepaald gebied ook een enquete kunnen worden gehouden waarbij aan mensen wordt gevraagd welke beveiliging ze gebruiken, wat ze hierover weten, waarom ze een bepaalde beveiliging gebruiken, etc. Met zo een soort onderzoek kan meer naar de houding van mensen tegenover beveiliging van draadloze netwerken worden gekeken. Het gedrag van mensen ten opzichte van beveiliging van draadloze netwerken kan dan goed in kaart worden gebracht.

Literatuur

Hieronder wordt de literatuur weergegeven, die gebruikt is bij het uitvoeren van dit onderzoek en bij het opstellen van deze master thesis.

[1] Albrecht, K.; Dutch Broadband Q4; Onderzoeksrapport; Telecompaper; 11 maart 2009

[2] Berghel, H.; Wireless Infidelity I: War Driving; *Communications of the ACM*; September 2004/Vol. 47, No. 9; pp. 21-26; 2004

[3] Consumentenbond; Dossier draadloos internet; *Digitaalgids*; Jaargang 2008/6 November/December; pp. 10-16; 2008

[4] Cracknell, P., Gavrilenko, K. & Vladimirov, A.; The Wireless Security Survey of London, 7th Edition; White Paper; RSA, The Security Division of EMC; 2008

[5] Cracknell, P., Gavrilenko, K. & Vladimirov, A.; The Wireless Security Survey of New York City, 4th Edition; White Paper; RSA, The Security Division of EMC; 2008

[6] Cracknell, P., Gavrilenko, K. & Vladimirov, A.; The Wireless Security Survey of Paris, 4th Edition; White Paper; RSA, The Security Division of EMC; 2008

[7] Earle, A.E.; *Wireless Security Handbook*; Auerbach Publications; Boca Raton; 2006

[8] European Commission; E-Communications Household Survey; *Eurobarometer 293 / Wave 68.2 – TNS opinion & social*; June 2008

[9] Horrigan, J.; Wireless Internet Access; Data Memo February 2007; Pew Internet & American Life Project; 2007

[10] Hurley, C., Connelly, D., Baker, B., Rogers, R. & Thornton, F.; *WarDriving & Wireless Penetration Testing*; Syngress Publishing; Rockland; 2007

[11] Jaquith, A.; *Security Metrics: Replacing Fear, Uncertainty, and Doubt*; Pearson Education; Boston; 2007

[12] McClave, J.T., Benson, P.G. & Sincich, T.; *Statistiek, Een inleiding voor het hoger onderwijs*; Achtste editie; Pearson Education Benelux; 2003

[13] Molenaar, D.; Zorgplicht: voorlichting abonnees over draadloze routers; Openbare brief; Het college van de Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA); 5 maart 2009

[14] Nagamalai, D., Dhinakaran, B.C., Sasikala, P., Lee, S.-H. & Lee, J.-K.; Security Threats and Countermeasures in WLAN; *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; AINTEC 2005, 3837 LNCS; pp. 168-182; 2005

[15] Professional Information Security Association (PISA) & Hong Kong Wireless Technology Industry Association (WTIA); Report on Wireless LAN War Driving Survey 2004-05 Hong Kong; 2005

[16] Ross, J.; *The book of wireless 2nd Edition, A painless guide to wi-fi and broadband wireless*; No Starch Press; San Francisco; 2008

[17] Violettas, G.E., Theodorou, T.L., Chalkias, K. & Stephanides, G.C.; Surveying WI-FI security - Presentation of Wi-Fi security measures, varius Wi-Fi attacks and a classification survey of Wi-Fi Networks in Thessaloniki; *WINSYS 2008 - International Conference on Wireless Information Networks and Systems, Proceedings*; pp. 96-101; 2008

[18] Wong, M., Clement, A.; Sharing Wireless Internet in Urban Neighbourhoods; Working Paper No. 19; Canadian Research Alliance for Community Innovation and Networking (CRACIN); 2007

Bijlagen

Hieronder worden de bijlagen die horen bij deze master thesis, weergegeven.

Bijlage 1: Kruistabellen

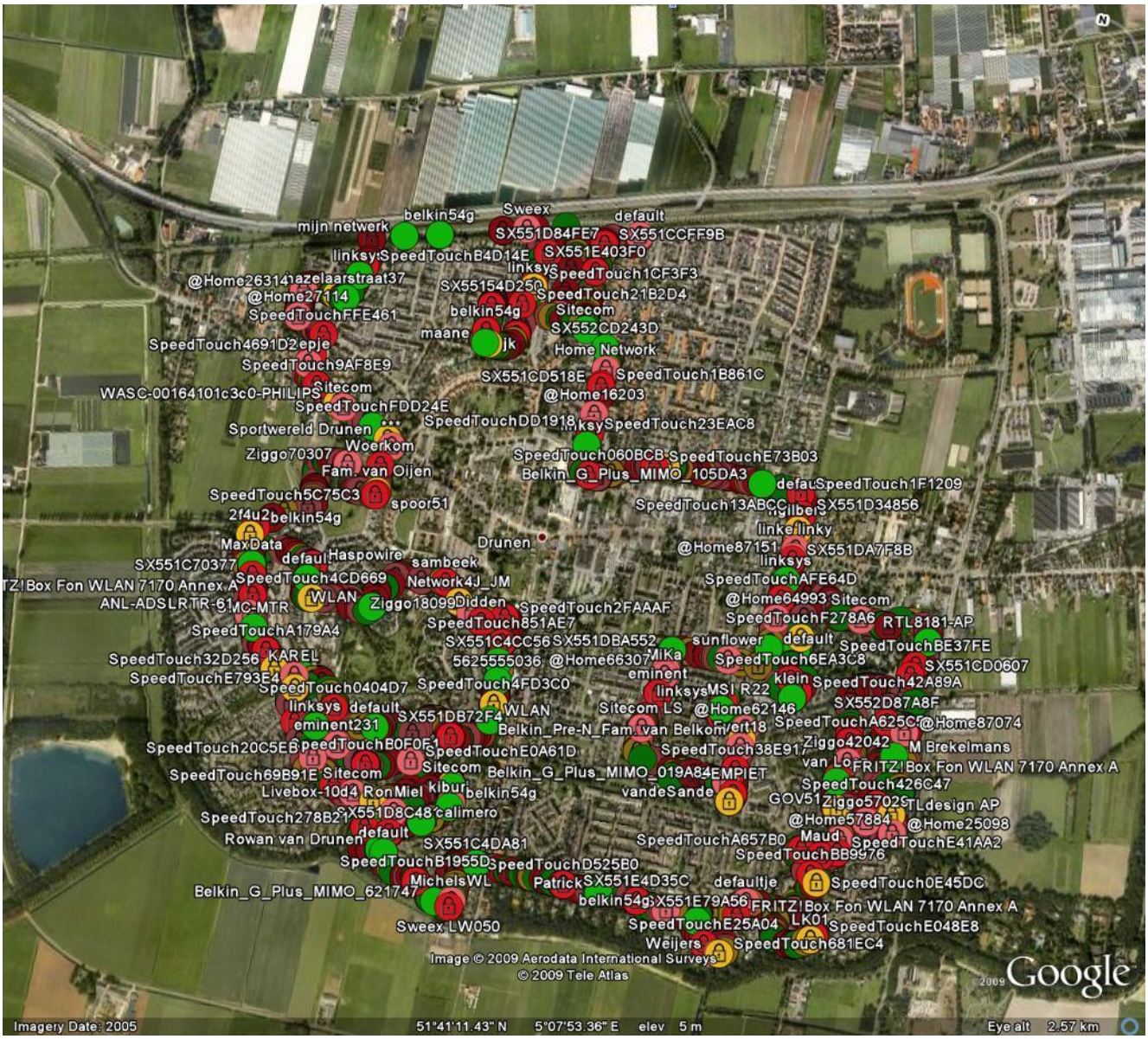
Kruistabel 1 (Encryptieniveau * Routermerk Crosstabulation)

			Routermerk														
			AMIT	ASUSTek	AVM	Belkin	Cisco-Linksys	D-Link	Eminent	Netgear	Siemens	Sitecom	SMC	SWEEX	Thomson	ZyGate	**Total**
Encryptie-niveau	None	Count	8	10	0	13	42	2	1	6	1	37	5	6	6	1	**138**
		% within Merk	15,7%	27,0%	,0%	9,9%	14,3%	7,1%	2,9%	3,8%	,5%	20,2%	20,8%	16,7%	1,4%	4,5%	**8,3%**
		% of Total	,5%	,6%	,0%	,8%	2,5%	,1%	,1%	,4%	,1%	2,2%	,3%	,4%	,4%	,1%	**8,3%**
	WEP	Count	23	9	0	55	96	10	17	8	33	56	8	12	73	7	**407**
		% within Merk	45,1%	24,3%	,0%	42,0%	32,8%	35,7%	50,0%	5,1%	15,9%	30,6%	33,3%	33,3%	17,0%	31,8%	**24,6%**
		% of Total	1,4%	,5%	,0%	3,3%	5,8%	,6%	1,0%	,5%	2,0%	3,4%	,5%	,7%	4,4%	,4%	**24,6%**
	WPA	Count	20	5	0	31	101	7	13	129	1	65	5	6	34	8	**425**
		% within Merk	39,2%	13,5%	,0%	23,7%	34,5%	25,0%	38,2%	82,2%	,5%	35,5%	20,8%	16,7%	7,9%	36,4%	**25,7%**
		% of Total	1,2%	,3%	,0%	1,9%	6,1%	,4%	,8%	7,8%	,1%	3,9%	,3%	,4%	2,1%	,5%	**25,7%**
	WPA2	Count	0	13	20	32	54	9	3	14	172	25	6	12	317	6	**683**
		% within Merk	,0%	35,1%	100,0%	24,4%	18,4%	32,1%	8,8%	8,9%	83,1%	13,7%	25,0%	33,3%	73,7%	27,3%	**41,3%**
		% of Total	,0%	,8%	1,2%	1,9%	3,3%	,5%	,2%	,8%	10,4%	1,5%	,4%	,7%	19,2%	,4%	**41,3%**
Total		**Count**	**51**	**37**	**20**	**131**	**293**	**28**	**34**	**157**	**207**	**183**	**24**	**36**	**430**	**22**	**1653**
		% within Merk	**100,0%**	**100,0%**	**100,0%**	**100,0%**	**100,0%**	**100,0%**	**100,0%**	**100,0%**	**100,0%**	**100,0%**	**100,0%**	**100,0%**	**100,0%**	**100,0%**	**100,0%**
		% of Total	**3,1%**	**2,2%**	**1,2%**	**7,9%**	**17,7%**	**1,7%**	**2,1%**	**9,5%**	**12,5%**	**11,1%**	**1,5%**	**2,2%**	**26,0%**	**1,3%**	**100,0%**

Kruistabel 2 (Routerconfiguratie * Routermerk Crosstabulation)

			Routermerk														
			AMIT	ASUSTek	AVM	Belkin	Cisco-Linksys	D-Link	Eminent	Netgear	Siemens	Sitecom	SMC	SWEEX	Thomson	ZyGate	**Total**
Router-configuratie	Stnd.	Count	15	6	15	52	87	7	16	127	167	130	15	24	369	0	**1030**
		% within Merk	29,4%	16,2%	75,0%	39,7%	29,7%	25,0%	47,1%	80,9%	80,7%	71,0%	62,5%	66,7%	85,8%	,0%	**62,3%**
		% of Total	,9%	,4%	,9%	3,1%	5,3%	,4%	1,0%	7,7%	10,1%	7,9%	,9%	1,5%	22,3%	,0%	**62,3%**
	Niet Stnd.	Count	36	31	5	79	206	21	18	30	40	53	9	12	61	22	**623**
		% within Merk	70,6%	83,8%	25,0%	60,3%	70,3%	75,0%	52,9%	19,1%	19,3%	29,0%	37,5%	33,3%	14,2%	100,0%	**37,7%**
		% of Total	2,2%	1,9%	,3%	4,8%	12,5%	1,3%	1,1%	1,8%	2,4%	3,2%	,5%	,7%	3,7%	1,3%	**37,7%**
Total		**Count**	**51**	**37**	**20**	**131**	**293**	**28**	**34**	**157**	**207**	**183**	**24**	**36**	**430**	**22**	**1653**
		% within Merk	**100,0%**	**100,0%**	**100,0%**	**100,0%**	**100,0%**	**100,0%**	**100,0%**	**100,0%**	**100,0%**	**100,0%**	**100,0%**	**100,0%**	**100,0%**	**100,0%**	**100,0%**
		% of Total	**3,1%**	**2,2%**	**1,2%**	**7,9%**	**17,7%**	**1,7%**	**2,1%**	**9,5%**	**12,5%**	**11,1%**	**1,5%**	**2,2%**	**26,0%**	**1,3%**	**100,0%**

Bijlage 2: War Driving GPS Map



Legenda

= GEEN

= WEP

= WPA

= WPA2

Bijlage 3: ISP Vragenlijst

Geachte heer/mevrouw,

Ik ben in opdracht van de Radboud Universiteit in Nijmegen bezig met een onderzoek naar de veiligheid van draadloze Wi-Fi netwerken bij particulieren in Nederland. Graag wil ik u een aantal vragen stellen over hoe u als Internet Service Provider omgaat met de beveiliging van deze draadloze Wi-Fi thuisnetwerken. De vragen komen hieronder één voor één aan bod.

1. Welk merk draadloze Wi-Fi modem/router levert u aan de consumenten?
2. Kunt u mij de aansluitingsprocedure (handleiding voor aansluiting) van deze draadloze Wi-Fi modem/router mailen of opsturen?
3. Geeft u als Internet Service Provider voorlichting aan uw klanten betreffende de beveiliging van draadloze Wi-Fi thuisnetwerken? Zo ja, hoe?
4. Heeft u als Internet Service Provider maatregelen genomen naar aanleiding van de door OPTA ingevoerde informatieplicht betreffende onveilig ingestelde draadloze Wi-Fi modems/routers bij consumenten van 5 maart 2009? Zo ja, welke?
5. Wat bent u als Internet Service Provider van plan om in de toekomst te doen op het gebied van beveiliging van draadloze Wi-Fi thuisnetwerken met betrekking tot voorlichting en/of de aansluitingsprocedures van draadloze Wi-Fi modems/routers?

Het onderzoek zal begin juli worden afgerond. De onderzoeksresultaten worden, indien u dit wenst, aan u beschikbaar gesteld. Alvast bedankt voor uw medewerking.

Met vriendelijke groeten,

Zlatko Bajić
Digital Security Group
Radboud Universiteit Nijmegen
z.bajic@student.ru.nl

Thuisadres:
Barentszstraat 16
5151 MC Drunen