Bachelorscriptie
Informatica

Radboud Universiteit

Vakdidactische aspecten van security

Auteur:
Petra van den Bos
petravandenbos@student.ru.nl

Inhoudelijk begeleider:
Erik Barendsen

Tweede lezers:
Erik Poll
Marko van Eekelen

11 juli 2013

Samenvatting

In deze bachelorscriptie wordt geïnventariseerd hoe security onderwezen wordt in het huidige onderwijs. Het concept *Pedagogical Content Knowlegde* biedt hier een raamwerk voor. *Pedagogical content knowlegde* is de kennis van docenten over hoe je een onderwerp aan leerlingen leert. De resultaten die dit onderzoek oplevert, worden gebruikt voor de ontwikkeling voor een module over security.

Inhoudsopgave

1 Inleiding

Security is een onderwerp dat maar zelden aan bod komt op middelbare scholen in Nederland. Meer algemeen valt er nog wel wat te verbeteren aan het onderwijs in Informatica, zoals ook blijkt uit het advies van de KNAW (Koninklijke Nederlandse Akademie van Wetenschappen, 2012). Het advies gaat over de digitale geletterdheid die iedere burger zou moeten hebben. Er worden relatief veel onderwerpen genoemd die security-gerelateerd zijn. Het advies noemt dat het huidige bovenbouwvak Informatica slechts door 5% van de leerlingen gevolgd wordt. Bovendien gaat het vak over *computers, programma's, systemen en bedrijfstoepassingen.* Als security al aan bod komt bij deze onderwerpen, zal dat niet uitgebreid zijn.

De nieuwe vakken die het advies adviseert zijn nog niet gerealiseerd. Voorlopig zullen we het moeten doen met de huidige vakken. In 2007 is er een nieuw bètavak ingevoerd: Natuur, Leven en Technologie (Landelijk Coördinatiepunt NLT, 2013), afgekort NLT. Bij het laatste woord, *Technologie*, past security prima. In de security worden vele technieken gebruikt om een bepaald soort beveiliging te realiseren. Security heeft ook zeker maatschappelijke kanten, waardoor het ook aansluit bij het woord *Leven*. NLT is opgebouwd uit modules: op zichzelf staande hoofdstukken waarmee een school een eigen programma kan samenstellen. Een module over security zou dus prima binnen dit vak passen.

De Radboud Universiteit Nijmegen heeft een afdeling *Digital Security Group*, speciaal gericht op security. Docenten van deze afdeling verzorgen onderwijs over security voor de opleiding Informatica. Komend jaar wordt zelfs gestart met een bachelor-track *Cybersecurity* voor de studie Informatica . Bovendien komt security bij verschillende voorlichtingsactiviteiten (masterclasses, 4 VWO-dagen, proefstudeerdagen) over de studie vaak aan bod. Hierdoor is er al veel materiaal beschikbaar dat geschikt is voor middelbare scholieren. Ook is er al eerder een module gemaakt voor NLT, namelijk over Robotica. Verder verzorgt de universiteit ook zelf NLT-onderwijs. Middelbare scholieren van scholen uit de buurt komen dan voor een middag naar de universiteit om aan dit onderwijs deel te nemen. Deze achtergrond en ervaring biedt dus een goede basis voor het ontwikkelen van een module over security voor NLT.

Deze scriptie zal een verantwoording vormen voor de module. Het concept *Pedagogical Content Knowledge* zal hierbij een centrale rol spelen. De grondlegger van dit concept, Shulman (1986), formuleert deze vorm van kennis als volgt: 'the ways of representing and formulating the subject that make it comprehensible to others'. *Pedagogical Content Knowledge* is dus kennis over de manier(en) om een onderwerp op een zo goed mogelijke wijze over te brengen aan leerlingen. Deze kennis is precies wat er nodig is om een goede module te ontwikkelen.

In *Probleemstelling* zal met behulp van *Pedagogical Content Knowledge* de onderzoeksvraag uitgewerkt worden. Vervolgens zal in *Theoretisch kader* dieper worden ingegaan op *Pedagogical Content Knowledge* en op theorie over onderwijsmethoden. Daarna zal in *Methode* besproken worden welke methodes gebruikt zijn om de onderzoeksvraag te beantwoorden door verschillende bronnen te analyseren. Vervolgens zullen de analyses van die bronnen in *Resultaten* uiteengezet worden. Al deze resultaten zullen in *Conclusies en Discussie* samengevoegd en vergeleken worden. Hierbij zal besproken worden wat dit betekent voor de ontwikkeling van de module.

2 Probleemstelling

2.1 Onderzoeksvraag

Zoals in *Inleiding* al gezegd is, zal deze scriptie een verantwoording vormen voor het ontwikkelen van een module over security. *Pedagogical Content Knowledge* gaat over de vakdidactische kennis van docenten, maar net zoals in (Saeli, 2012) zullen de onderdelen van *Pedagogical Content Knowledge* gebruikt worden om in het algemeen iets te zeggen over het onderwijzen van security, omdat die onderdelen een goede leidraad bieden.

Er is nog nooit een echt onderzoek gedaan naar het onderwijzen van security, omdat security een relatief nieuw vakgebied is. Deze scriptie zal daarom een begin maken met het in kader brengen van de verschillende manieren om onderwijs te geven over security. Verder onderzoek zal moeten uitwijzen wat in het algemeen goede manieren zijn om security te onderwijzen.

Onderzoeksvraag: Hoe wordt security onderwezen in het huidige onderwijs?

Vervolgvraag: Hoe kunnen de resultaten gebruikt worden voor de ontwikkeling van de module?

De onderzoeksvraag is redelijk algemeen, daarom zal dit concreter worden gemaakt met een aantal deelvragen. Aan de hand van de antwoorden op deze deelvragen kan worden ingegaan op de vervolgvraag. Magnusson, Krajcik en Borko (1999) hebben in hun paper (Magnusson et al., 1999) *Pedagogical Content Knowledge* uitgewerkt in een aantal onderdelen. Zoals hiervoor gezegd, worden deze onderdelen in deze scriptie gebruikt om onderwijs in het algemeen te onderzoek i.p.v. de kennis van één docent. De onderdelen zijn:

- kennis over het curriculum,
- kennis over het begrip van leerlingen over het onderwerp,
- manieren of methodes om het onderwerp te onderwijzen, en
- methodes om te toetsen wat de leerlingen geleerd hebben over het onderwerp.

Op deze onderdelen zijn onderstaande deelvragen gebaseerd. In *Theoretisch kader* wordt verder ingegaan op de onderdelen zoals ze in de paper aan bod komen.

Deelvragen:

1. Wat zijn mogelijke leerdoelen van security en waarom zou een leerling dit moeten leren?

   Een leerdoel beschrijft het beoogde leerresultaat. Een leerdoel beschrijft vaak een (algemeen) onderwerp en een niveau waarop de leerling dit onderwerp moet beheersen. In *Theoretisch kader* wordt uitgebreider ingegaan op (de verschillende soorten) leerdoelen.

   Bij de leerdoelen hoort ook een verantwoording: waarom zou de leerling dit moeten leren? Deze redenen leggen bijvoorbeeld uit waarom een bepaald leerdoel past bij security, waarom het (maatschappelijk) relevant is dat de leerling dit leert, of waarom het bijdraagt aan de ontwikkeling van de leerling.

2. Welk begrip hebben de leerlingen van security?

   Het begrip van leerlingen wordt voornamelijk bepaald door de voorkennis die ze hebben en de problemen die ze tegen komen tijdens het leren. Daarom is het belangrijk om vast te leggen welke voorkennis nodig is, zodat ieder die het onderwijs volgt weet wat hij/zij al eerder geleerd moet hebben. In het onderwijs zelf wordt vaak weinig aandacht aan die vereiste voorkennis besteed, maar er wordt wel op voortgebouwd. Als de problemen van leerlingen bekend zijn kan het onderwijs daarop aangepast worden, waardoor de problemen opgelost of omzeild worden in plaats van dat de leerlingen ermee blijven zitten.

3. Welke aanpakken zijn er om security te onderwijzen?

   Er zijn vele manieren om een onderwerp te onderwijzen. Er kunnen verschillende begrippen gebruikt worden, er kan eerst begonnen worden met de theorie of eerst met een voorbeeld, er wordt eerst een algemeen beeld geschetst of er wordt juist met de details begonnen. Maar ook de volgorde van de onderwerpen, de schrijf- of spreekstijl en de werkwijze (zelfstandig, in groepjes, verhouding theorie en opdrachten) horen hierbij.

4. Op welke manieren kan het behalen van de leerdoelen getoetst worden?

   Het is wel de bedoeling dat de leerdoelen die bij de module horen ook daadwerkelijk behaald worden. Daarom moet zowel tussendoor als op het einde gecontroleerd worden of de leerlingen ook echt wat geleerd hebben. Dit hoeft niet altijd een formele toets te zijn. Ook gemaakte opdrachten of de beantwoording van een gestelde vraag kunnen helpen om vast te stellen of de leerdoelen gehaald zijn.

2.2 Context

De module waarvoor deze scriptie een verantwoording vormt, wordt ontwikkeld voor het middelbare schoolvak NLT. Bij het ontwikkelen van de module moet hiermee rekening gehouden worden. Vanuit NLT zijn er namelijk een aantal doelstellingen, criteria en procedures opgesteld, die van toepassing zijn op de module.

De website van NLT (Landelijk Coördinatiepunt NLT, 2013) verstrekt allerlei informatie over het vak. Deze website is opgezet door het Landelijk Cordinatiepunt NLT, het uitvoerend orgaan van de Stuurgroep NLT. Op de website is het Visiedocument (Stuurgroep Natuur, Leven en Technologie, 2007) te vinden die de informatie over NLT bundelt. Te lezen is dat NLT in 2007 is ingevoerd als nieuw, geïntegreerd bètavak met als doel het verhogen van de aantrekkelijkheid van bètaonderwijs en het versterken van samenhang tussen bètavakken.

Voor het ontwikkelen van modules zijn bepaalde procedures (*Procedure ontwikkelen en certificeren externe NLT-modules*, 2012). De meeste modules worden ontwikkeld in opdracht van het Landelijk Ontwikkelpunt NLT (de voorganger van het Landelijk Coördinatiepunt NLT). Ook worden er extern modules ontwikkeld. Tot die groep gaat de module over security behoren. Externe modules moeten wel voldoen aan bepaalde procedurele en inhoudelijke criteria (bijlage 2 en 3 van (*Procedure ontwikkelen en certificeren externe NLT-modules*, 2012)) voldoen om gecertificeerd te worden.

Enkele inhoudelijke criteria zijn: de module moet actueel zijn, de module moet passen in het examenprogramma (Minister van Onderwijs, Cultuur en Wetenschap, 2011), concepten worden behandeld in context, de omvang van de module is 40 studielasturen, de module is geschikt voor vwo of havo leerlingen, de module bevat leerdoelen, docentenmateriaal en toetsmateriaal, en de module moet in meerdere regio's en scholen te gebruiken zijn.

Volgens de procedurele criteria moet de module getest zijn door (in principe twee) onafhankelijke scholen. Deze scholen mogen niet bij de ontwikkeling van de module betrokken geweest zijn. De test beoordeeld in ieder geval de haalbaarheid qua niveau en tijd voor de beoogde doelgroep. Verder moet de module ook door een expert beoordeeld worden. Deze expert mag ook niet bij de ontwikkeling betrokken geweest zijn. Hij beoordeeld in ieder geval de correctheid en de actualiteit van de module.

Er is onderzoek (Rouwenhorst, Praagman, Stevens, Wagner & Griffioen, 2010) gedaan naar de invloed van NLT op de cijfers van andere bètavakken en de overdracht van kennis tussen NLT en de bètavakken. Uit het relatief kleinschalige onderzoek volgt dat er geen duidelijk meetbaar effect is (qua cijfers), al vinden de proefpersonen wel dat NLT iets bijdraagt. Dat er geen meetbaar effect is hoeft niet te betekenen dat er geen invloed of overdracht is. Er worden een aantal mogelijke redenen gegeven, waaronder dat mensen die NLT kiezen misschien toch al goed waren in de andere bètavakken.

3 Theoretisch kader

3.1 Pedagogical Content Knowledge

In (Magnusson et al., 1999) wordt beschreven wat *Pedagogical Content Knowlegde* is en welke onderdelen te onderscheiden zijn. Er wordt genoemd dat de *Pedagogical Content Knowlegde* van een docent datgene is wat een docent van een specialist onderscheidt. *Pedagogical Content Knowlegde* combineert dus de kennis van het vakgebied met de kennis over de methodes om de kennis over te brengen, ofwel didactiek. Hieronder wordt ingegaan op de onderdelen en subonderdelen, zoals gepresenteerd in (Magnusson et al., 1999). In deze onderdelen zijn de deelvragen te herkennen. In deze scriptie worden de onderdelen van Magnusson et al. (1999), zoals eerder gezegd, breder opgevat, net zoals in (Saeli, 2012). Hierdoor gaan de onderdelen in het algemeen over onderwijs van security en dus niet alleen over docentkennis over dat onderwijs.

Het eerste onderdeel is de kennis van het curriculum. Bij dit onderdeel worden twee subonderdelen genoemd: specifieke curricula en doelstellingen. Doelstellingen geven een algemene richting, terwijl een specifiek curriculum al echt een programma met materialen vastlegt. Die kennis over het curriculum is niet zomaar ontstaan, daar is over nagedacht en meestal is het ook al in de praktijk uitgeprobeerd. Er bestaan dus redenen waarom voor bepaalde doelen of specifieke curricula is gekozen. De subonderdelen doelstellingen en specifieke curricula zijn beiden te beschrijven met leerdoelen. Als het over doelstellingen gaat, zullen de leerdoelen algemener zijn dan wanneer het over specifieke curricula gaat.

Het tweede onderdeel is de kennis van het begrip dat leerlingen hebben van het onderwerp. Ten eerste wordt dit begrip bepaald door de voorkennis van de leerling die nodig is om het onderwerp te begrijpen. Vaak wordt verondersteld dat de leerling al over bepaalde kennis beschikt als een onderwerp uitgelegd wordt. Bij de vereiste voorkennis zijn de leerstijlen die de leerlingen hebben aangeleerd inbegrepen. Ten tweede wordt dit begrip bepaald door de problemen of moeilijkheden die de leerlingen hebben bij het leren van het onderwerp. Als de problemen bekend zijn kan het onderwijs daarop inspelen.

Het derde onderdeel is kennis over strategieën om het onderwerp over te brengen, dus de onderwijsaanpak. Er zijn twee soorten strategieën: strategieën die toepasbaar zijn bij elk onderwerp en strategieën die alleen geschikt zijn voor bepaalde specifieke onderwerpen. De laatste soort strategieën is vaak een representatie of activiteit die het overbrengen van het onderwerp makkelijker maakt.

Het vierde onderdeel gaat over het beoordelen of toetsen van de opgedane kennis van leerlingen. Leerlingen leren verschillende onderwerpen soms op verschillende manieren, waardoor dat leren ook op verschillende manieren beoordeeld kan worden. Denk hierbij aan een (geschreven) tentamen, een (praktische) opdracht of een presentatie. Ook vindt het toetsen op verschillende momenten in het leerproces plaats, waardoor sommige methodes niet of juist wel geschikt zijn voor een bepaald moment.

3.2 Onderwijsmethoden

Het is belangrijk dat het onderwijs op een goede manier in elkaar zit. Er is hier al veel onderzoek naar gedaan. Hieronder zullen twee onderwerpen aan bod komen: Blooms taxonomie en het constructivisme.

3.2.1 Blooms taxonomie

Blooms taxonomie (Bloom, 1956) geeft weer welke categorieën van leren te onderscheiden zijn. Deze categorieën zijn niet allemaal even moeilijk, er zijn verschillende niveaus. Bovendien is een categorie van een hoger niveau afhankelijk van de categorieën van de lagere niveaus. De categorieën zie je vaak terug in leerdoelen. Een leerdoel beschrijft namelijk wat een leerling geleerd zou moeten hebben na het volgen van bepaald onderwijs. Daarom is het vaak mogelijk zo'n categorie te herkennen in een leerdoel. Andersom helpt de taxonomie van Bloom om goede

leerdoelen op te stellen, door na te denken bij welke categorie het leerdoel hoort. Ook helpt het om te zorgen dat de leerdoelen niet alleen over categorieën van de lagere niveaus gaan, maar ook de hogere niveaus. Hieronder volgt een beschrijving van de categorieën. Onderaan staat een tabel die de taxonomie grafisch weergeeft.

De categorie *Kennis* staat het laagst. Op dit niveau onthoudt de leerling de informatie. Hier wordt dan ook meestal mee begonnen in het onderwijs.

Als de kennis aanwezig is, kan er een niveau hoger worden gegaan naar *Inzicht*. Op dit niveau heeft de leerling begrip gevormd van het onderwerp, waardoor hij zaken kan vergelijken, interpreteren, uitbreiden etc.

Als de leerling begrijpt hoe het onderwerp in elkaar steekt, kan hij naar een volgend niveau: het toepassen. Als de leerling het niveau *Toepassing* beheerst, kan hij nieuwe kennis gebruiken, nieuwe problemen oplossen en de kennis toepassen op een andere manier.

Boven het niveau *Toepassing* staan drie categorieën op dezelfde hoogte: *Analyse*, *Synthese* en *Evaluatie*. Deze drie categorieën zijn van hetzelfde niveau. De categorie *Analyse* gaat over het onderzoeken en opsplitsen van bepaalde informatie, waarbij afleidingen gemaakt worden. Bij *Synthese* wordt informatie op een andere manier samengesteld of wordt een nieuwe oplossing aangedragen. Bij *Evaluatie* kan de leerling een oordeel geven over de waarde van bepaalde informatie, of over de correctheid van ideeën.

Analyse	Synthese	Evaluatie
	Toepassing	
	Inzicht	
	Kennis	

Tabel 1: Blooms taxonomie

3.2.2 Constructivisme

Met constructivisme wordt, in de context van onderwijsmethoden, een opvatting aangeduid over het proces van het leren. Volgens deze opvatting is leren geen passieve transmissie van kennis van de leraar naar de leerling, maar leert de leerling nieuwe kennis door deze actief te construeren uit datgene wat de leerling eerder geleerd heeft (Bransford, Brown, Cocking et al., 2000).

Als men deze manier van leren in het onderwijs wil ondersteunen, is het nodig om het onderwijs hierop aan te passen. Ten eerste is de leraar veel meer een gids die de leerling helpt dan iemand die zegt hoe het zit en dan ervan uit gaat dat leerlingen dit weten. Ten tweede moet de leraar er gebruik van maken dat het leren van leerlingen sterk beïnvloed wordt door de kennis die ze al eerder hebben opgedaan. De leerlingen zullen niet allemaal dezelfde voorkennis hebben, dus hier moet de leraar zich op aanpassen. Ten derde moet de leraar ook stimuleren dat leerlingen nieuwe dingen aan hun voorkennis koppelen. Ten vierde moet de leraar de leerling de tijd gunnen om de nieuwe kennis te construeren zodat de leerlingen de kans hebben na te denken en te reflecteren.

4 Methode

Er zijn verschillende bronnen gebruikt om de deelvragen en daarmee de onderzoeksvraag te beantwoorden. De eerste drie bronnen geven vooral een inhoudelijk beeld van security. De laatste twee bronnen zijn algemener.

4.1 Het vak Security

Op de Radboud Universiteit Nijmegen wordt het vak *Security* gegeven door Bart Jacobs. Zoals de naam al suggereert is het vak dus een specifieke vorm van onderwijs over security. Er zijn voor dit vak al keuzes gemaakt over hoe het onderwijs wordt vormgegeven. Dit maakt het vak een interessante bron om voor deze scriptie te gebruiken. Van het vak zijn vier bronnen beschikbaar: de studiegids (*Studiegids Security*, 2011), collegeslides (Jacobs, 2011c), assignments (Jacobs, 2011b) (iedere assignment bevat een aantal opdrachten) en een tentamen (Jacobs, 2011a).

In de studiegids wordt bijna letterlijk, maar kort, antwoord gegeven op de deelvragen. Met behulp van citaten worden dit besproken.

De collegeslides zijn doorgenomen, waarbij zo volledig mogelijk is nagegaan welke onderwerpen er in deze collegeslides behandeld worden. Hierbij is geprobeerd om de onderwerpen zo algemeen mogelijk te formuleren, maar zo dat toch duidelijk blijft wat voor specifieke dingen aan bod zijn gekomen. Hierdoor hoefde er niet voor elke slide een onderwerp genoemd te worden. De meeste onderwerpen besloegen wel een paar collegeslides. Maar als er veel kleine, verschillende onderwerpen genoemd werden, zijn deze toch genoteerd.

Doordat er voor dit vak vier bronnen beschikbaar zijn, biedt dit de mogelijkheid om ze met elkaar te vergelijken. Er worden twee vergelijkingen gedaan: de leerdoelen van de studiegids met de geïnventariseerde onderwerpen uit de collegeslides en vervolgens de geïnventariseerde onderwerpen met de onderwerpen die aan bod komen in de assignments.

De leerdoelen uit de studiegids zijn op een veel hoger niveau geformuleerd dan de onderwerpen die bij de inventarisatie gevonden zijn. Per leerdoel wordt aangegeven welke soorten of groepen onderwerpen bij dit leerdoel passen. Hiermee wordt duidelijk of de onderwerpen passen bij de leerdoelen. Er is niet precies aangegeven welke onderwerpen bij de leerdoelen horen, omdat de leerdoelen zo abstract zijn, dat het erg onduidelijk is welke onderwerpen wel en welke niet bij de leerdoelen horen.

Voor iedere opdracht van de assignments is vastgesteld welk onderwerp of welke onderwerpen in die opdracht aan bod komen. Dit is weergegeven met een tabel. Vervolgens is nagegaan of er onderwerpen zijn die niet aan bod komen in de opdrachten en andersom, of de opdrachten zijn die over een ander onderwerp gaan dan de onderwerpen van de collegeslides.

Als de geïnventariseerde onderwerpen ervoor zorgen dat de leerdoelen uit de studiegids ermee behaald kunnen en worden, en als de assignments ervoor zorgen dat de geïnventariseerde onderwerpen aan bod komen, betekent dit dat, indirect, de leerdoelen behaald worden met de assignments.

Tenslotte wordt van elke vraag uit het tentamen (Jacobs, 2011a) ingedeeld bij één van de categorieën van Blooms taxonomie. Hiermee wordt duidelijk welk niveau het tentamen heeft.

4.2 Enigma

Enigma is een lesmethode die bedoeld is voor het middelbare schoolvak Informatica. De methode is opgebouwd uit modules. Eén van die modules gaat over *Cryptografie*. De analyse van deze module is gebaseerd op het *Informatieboek*, het *Verwerkingsboek* en de *Toets* die bij deze module beschikbaar zijn gesteld.

Het *Informatieboek* is gebruikt om een inventarisatie te doen van de onderwerpen die aan bod komen. In het *Verwerkingsboek* worden leerdoelen opgesomd. Deze leerdoelen zijn vergeleken met de onderwerpen die gevonden zijn met de inventarisatie.

De leerdoelen uit het *Verwerkingsboek* zijn op een veel lager niveau geformuleerd dan de leerdoelen uit de studiegids van Security (*Studiegids Security*, 2011). Hierdoor is het voor deze leerdoelen

wel mogelijk om te bepalen welke onderwerpen precies bij de leerdoelen horen. Dit is in een tabel weergegeven. Vervolgens is er een analyse gedaan van deze tabel, door vanuit de leerdoelen en vanuit de onderwerpen in de tabel te zoeken naar opvallende aspecten, voornamelijk door naar de aantallen te kijken. Verder zijn de leerdoelen ingedeeld in de categorieën van Blooms taxonomie. Ook is van de opdrachten uit het *Verwerkingsboek* vastgesteld welke leerdoelen daarmee aan bod komen en de categorie van Blooms taxonomie die bij die opdracht past. Zo kan vastgesteld worden welke categorieën met de opdrachten getoetst worden. Ten slotte is van de vragen van de *Toets* vastgesteld onder welke categorie van Blooms taxonomie ze vallen.

4.3 Interview met docent

Om niet alleen schriftelijke bronnen te hebben, is er een interview gedaan met een docent. In (Loughran, Mulhall & Berry, 2004) wordt een onderzoeksinstrument gegeven waarmee de verschillende aspecten van de Pedagogical Content Knowledge van een docent bepaald kunnen worden. Dit onderzoeksinstrument wordt *CoRe* genoemd, een afkorting van *Content Representation*, dit is de manier waarop de inhoud ofwel het onderwerp gerepresenteerd wordt. Dit onderzoeksinstrument is gebruikt om een docent te interviewen over het onderwijzen van security.

CoRe bestaat uit een aantal vragen. De vragen gaan over een specifiek concept, idee of inzicht van het (algemene, grotere) onderwerp dat de docent aan de studenten wil leren. De vragen zijn ieder bij één van de vier onderdelen van Magnusson et al. (1999) ingedeeld.

Kennis van het curriculum:
1. Wat wilt u dat studenten leren over dit idee?
2. Waarom is het belangrijk dat studenten dit leren?
3. Wat weet u nog meer over dit idee wat de studenten niet hoeven te leren?

Kennis van het begrip dat leerlingen van het onderwerp hebben:
4. Welke problemen en beperkingen van studenten beïnvloeden uw onderwijs?
5. Welke manieren van denken van de studenten beïnvloeden uw onderwijs?

Onderwijsaanpak:
6. Wat zijn andere factoren die uw onderwijs beïnvloeden?
7. Wat zijn uw werkwijzen of methodes in uw onderwijs en waarom gebruikt u deze methoden bij het onderwijzen van dit idee?

Het toetsen van de opgedane kennis van leerlingen:
8. Hoe stelt u vast in welke mate studenten het idee begrepen hebben?

Deze bovengenoemde vragen zijn best abstract, dus zal de geïnterviewde niet altijd meteen een antwoord klaar hebben. Ook hangen de vragen samen, waardoor je makkelijk overgangen kan maken van de ene vraag naar de andere vraag, dus het is verstandig hiervan gebruik te maken. Vanuit deze gedachtes is de volgende voorbereiding gemaakt:

Er wordt begonnen met een introductie over het doel van het interview: *In dit interview gaan we het hebben over het leren van security aan studenten.* Vervolgens moet er ergens een aanknopingspunt gevonden worden over de ideeën van het onderwerp die de geïnterviewde doceert. De eerste vraag die geteld wordt is: *Wat vind je belangrijk dat studenten leren?* Als daar geen antwoord op komt, kan gevraagd worden naar de vakken die de geïnterviewde geeft. Daar heeft de geïnterviewde zeker een antwoord op. Om meer te weten te komen over deze ideeën, kunnen de vragen *Welke deelgebieden kun je onderscheiden?* en *Wat moeten mensen zich later herinneren?* worden gesteld. Vervolgens kan voor de genoemde ideeën worden ingaan op de vragen zoals ze hierboven genoemd worden. Tijdens het stellen van deze vragen komen misschien nog nieuwe ideeën naar boven.

Bij het stellen van bovengenoemde vragen kan gebruik worden gemaakt van de samenhang van de vragen. Zo kunnen vraag 1 en 3 gecombineerd worden door gelijk te vragen wat de studenten

wel en niet hoeven te leren, want door de vraag zo te stellen zoekt de geïnterviewde de grens op. Vanaf vraag 1 kan er doorgegaan worden naar vraag 4, want als er is vastgesteld wat de studenten leren, is het makkelijker om te zeggen welk onderdeel studenten moeilijk vinden. Vanaf vraag 4 kan er een bruggetje gemaakt worden naar vraag 5 door algemener in te gaan op de manieren van denken.

Ook kan er vanaf vraag 1 doorgegaan worden naar vraag 7, want als is vastgesteld wat studenten leren, is het makkelijker om te bedenken welke onderwijsmethodes je gebruikt om de genoemde dingen aan studenten te leren. Vraag 7 is een prima aanknopingspunt voor vraag 8, want de methodes om onderwijs te geven zijn vaak gekoppeld aan de methodes om studenten te toetsen op wat ze geleerd hebben.

Met deze voorbereiding is een docent geïnterviewd die onderwijs over security geeft. Het geluid van dit interview is opgenomen. Daarna is het interview uitgeschreven met behulp van het opgenomen geluid. Hierbij zijn haperingen, stiltes en bevestigende woorden als *Ja* weggelaten. De verkregen tekst is opgedeeld in delen die over gaan over één vraag en één onderwerp. Elk van die delen is vervolgens bij één van de hierboven genoemde vragen gezet, samen met een kopje dat aangeeft waar dat deel over gaat. In de delen zijn de vragen die de interviewer stelde vaak weggelaten, een enkele keer is de vraag verwerkt in de eerste zin van dat stukje. Een paar zinnen van de geïnterviewde die niets toevoegden zijn ook weggelaten. Ten slotte is bij elke vraag een samenvatting toegevoegd van de delen die bij de vraag vermeld staan. Deze samenvatting geeft zo een korter en bondiger antwoord op de vraag.

4.4 Visiedocument

Bij de oprichting van het vak NLT is er een Visiedocument (Stuurgroep Natuur, Leven en Technologie, 2007) gemaakt. Hierin wordt, zoals de naam al zegt, een visie gegeven over het onderwijs van het vak NLT. Aangezien de module over security voor NLT bedoeld is, is dit een prima bron om ideeën over onderwijs uit te halen, ook al gaat het document niet specifiek over security. Twee onderdelen van het document sluiten aan op de deelvragen: het onderdeel *3.1 Kenmerken van het lesmateriaal* en het onderdeel *4.2 Toetsvormen*. Er worden ook domeinen gegeven voor het examenprogramma, maar die komen niet overeen met het examenprogramma dat later is uitgegeven (Minister van Onderwijs, Cultuur en Wetenschap, 2011). Bovendien zijn de domeinen in genoemde bronnen veel te algemeen, waardoor deze niet van toepassing zijn op onderwijs over security.

Het eerste onderdeel geeft een aantal kenmerken waaraan een module moet voldoen om te passen binnen het vak NLT. Het vierde kenmerk geeft een motivatie waarom ICT binnen NLT past. Deze motivatie wordt aan security gekoppeld door het verband te leggen met de ICT-aspecten die er genoemd worden.Het laatste kenmerk geeft een kader waarbinnen onderwerpen van een NLT-module moeten vallen. De overige kenmerken gaan allemaal over een bepaald aspect van de onderwijsaanpak die gebruikt wordt in een NLT-module.

Het tweede onderdeel stelt een aantal toetsvormen voor. Van de laatste toetsvorm worden een aantal concrete vraagtypen genoemd. Deze vraagtypen zijn in te delen bij de categorieën van Blooms taxonomie. Deze indeling is per vraagtype uitgewerkt. Daarna wordt de indeling gebruikt om een conclusie te trekken over de kwaliteit en validiteit van deze vraagtypen.

4.5 KNAW

Zoals al eerder gezegd, is het doel van het advies (Koninklijke Nederlandse Akademie van Wetenschappen, 2012) om de digitale geletterdheid van de burger stimuleren. Een van de aanbevelingen om in de praktijk dichter bij dit doel te komen is om het vak Informatie & communicatie in te voeren. Veel van de onderwerpen die bij dit vak genoemd worden zijn security-gerelateerd. Die gerelateerdheid zal beargumenteerd worden met behulp van (Jacobs, 2011c), (Jacobs, 2011b), (Anderson, 2008), (Enigma, 2013) en het *Interview*. De onderwerpen die security-gerelateerd zijn, vormen mogelijke leerdoelen van security.

Behalve (Anderson, 2008) worden alle bronnen, die gebruikt worden om security-gerelateerdheid aan te tonen, geanalyseerd in *Resultaten*, waardoor ze een solide basis vormen om dit mee te beoordelen. De reden dat het boek *Software Engineering* van Anderson (2008) gebruikt wordt, is omdat het boek het meest complete overzicht geeft van het vakgebied security. Zo kan ook van onderwerpen die niet in *Resultaten* voorkomen, aangetoond worden dat ze security-gerelateerd zijn. Veel boeken gaan maar op een deelgebied in, bijvoorbeeld cryptografie of access control. Op de website waar je het boek kunt downloaden (http://www.cl.cam.ac.uk/ rja14/book.html) wordt het boek aangeprezen door drie mensen (Don Norman, Gary McGraw en Bruce Schneier). Ze vinden het niet alleen een goed boek, maar benadrukken vooral dat het boek het vakgebied zo goed dekt. Verder wordt het boek vaak geciteerd op Google Scholar, 2023 keer op het moment van schrijven. Bovendien is er het simpele feit dat het boek is uitgegeven, wat aangeeft dat het aan enige kwaliteitseisen voldoet. Dit boek vormt daarom ook een solide basis om security-gerelateerdheid mee te beoordelen.

4.6 Vergelijking van resultaten

Nadat de bronnen één voor één geanalyseerd zijn, worden ze per deelvraag met elkaar vergeleken. Zo ontstaat er een beter overzicht van de resultaten. Doordat de resultaten per deelvraag vergeleken worden, zorgt dit ook voor een opstapje naar de conclusie.

4.7 Beantwoording onderzoeksvraag

Ten slotte wordt een conclusie getrokken over de onderzoeksvraag door per deelvraag te kijken wat de resultaten bijdragen aan de beantwoording van die deelvragen. Daarna wordt ingegaan op hoe de opgedane kennis gebruikt zal worden bij het ontwikkelen van de module.

5 Resultaten

5.1 Het vak Security

Op de Radboud universiteit Nijmegen wordt het vak *Security* gegeven door Bart Jacobs. Eerst zal op basis van de studiegids (*Studiegids Security*, 2011) van dit vak kort antwoord gegeven worden op de deelvragen. Daarna volgt een inventarisatie van de onderwerpen die in de collegeslides (Jacobs, 2011c) staan. Deze onderwerpen zullen vergeleken worden met de leerdoelen uit de studiegids en de onderwerpen die in de opdrachten aan bod komen. Ten slotte wordt van elk van de vragen van het tentamen (Jacobs, 2011a) bepaald in welke categorie van Blooms taxonomie de vraag valt.

5.1.1 Studiegids

De leerdoelen worden in de studiegids (*Studiegids Security*, 2011) als volgt beschreven:
'At the end of this course:

1. You are able to recognise – in society in general and within a job environment in particular – situations in which information security plays a role.
2. You are able to recognise relevant security goals in such situations (confidentiality, integrity, availability, authenticity, non-repudiation, accountability).
3. You can (on a global level) describe basic techniques to achieve these security goals, evaluate existing solutions, and propose new solutions in practical situations.
4. You recognise the social and organisational implications of security technologies (especially privacy), and you can take these aspects into account in your analysis of practical situations.'

Samengevat gaat het eerste leerdoel over situaties waarbij security een rol speelt, het tweede leerdoel over de security doelen, het derde leerdoel over technieken en het vierde leerdoel over de gevolgen van securitytechnologieën. Eerst zal ingegaan worden op de categorieën van Blooms taxonomie waarbinnen de leerdoelen vallen. Daarna zullen met behulp van de deelvragen de andere delen van de studiegids besproken worden.

Het woord *recognize* van het eerste leerdoel geeft een duidelijke indicatie dat dit leerdoel binnen de categorie *Kennis* valt. Al moet je die herkenning wel doen bij nieuwe situaties, waardoor het leerdoel ook wel aansluit bij de categorie *Toepassing*. Voor het tweede doel geldt hetzelfde.

Het derde leerdoel bestaat uit drie delen. Het beschrijven van de technieken die je geleerd hebt past duidelijk bij de categorie *Kennis*. Het evalueren van bestaande oplossingen, past duidelijk bij de categorie *Evaluatie*. Het voorstellen van een nieuwe oplossing is typisch voor de categorie *Synthese*.

Het vierde leerdoel bestaat uit twee delen. Om te kunnen inzien wat de gevolgen zijn van security-technologieën moet er toch minstens *Inzicht* gebruikt worden. Als het echt om nieuwe situaties gaat is het *Toepassing*. Het tweede deel van het leerdoel geeft met het woord *analysis* al aan dat dit deel past bij de categorie *Analyse*.

Alle categorieën komen met deze leerdoelen aan bod, wat aangeeft dat deze leerdoelen niet te oppervlakkig zijn. Met deze leerdoelen kunnen de leerlingen dus op alle niveaus proberen getoetst worden.

De studiegids noemt een algemene rede om onderwijs te geven over security: 'Security is widely recognized as being of great importance in all areas of information technology: networks, operating systems, databases etc.'.

De vereiste voorkennis wordt beschreven met 'Basic knowledge of computer science and mathematics (esp. algebra).'. Studenten hebben deze kennis kunnen opdoen in het eerste jaar omdat het vak gegeven wordt in het eerste semester van het tweede of derde jaar: 'Students may choose to take this course either in their second or in their third year (to make room for courses of the minor).'.

De onderwijsaanpak die gebruikt wordt bij dit vak staat wel kort beschreven, in termen van de activiteiten die plaatsvinden en regels die gelden. Er wordt hierbij ook deels ingegaan op de

toetsing van het vak: 'The course consists of weekly lectures and exercises. The exercises are compulsory, and make up half of your final mark. Exercises may be done in pairs. Your solution has to be handed in on paper before the deadline, at in the mailbox of your exercise course teacher on the 2nd floor of the Huygens building. Exercises not handed in in time will be graded 1; submission by e-mail or Blackboard is not accepted. Copying or stealing work from others or from the Web will result in all involved parties failing the course and notification of the exam committee, so make sure we don't discover anything if you copy yourself, and secure your own work against copying by others.'. Verder wordt er ook vermeldt welke literatuur gebruikt wordt: 'The slides used in the lectures form the basis of the course.'.

Hierboven staat al dat de student voor elke opdracht een cijfer krijgt. De toetsing voor het hele vak wordt als volgt beschreven: 'The examination will be based on the outcome of both the exercises and the written exam. If both parts (exercises and exam) of the examination have been completed in time, the final mark will be the average of the two, provided the outcome of the exams is at least 5.0. If the result of the exam is lower than 5.0, the final mark will be equal to this result.'.

5.1.2 Inventarisatie van onderwerpen

Hieronder staat een lijst met onderwerpen per set slides van de collegeslides (Jacobs, 2011c).

Introduction

1. Wat security is en hoe dit in de maatschappij tot uiting komt.
2. De security doelen.
3. Wat protocollen zijn (met bijbehorende notatie).
4. Veiligheid van protocollen.

Symmetric crypto

5. Wat Symmetrische cryptografie is.
6. Het vercijferen en ontcijferen met een simpele (symmetrische) cryptografische methode.
7. De zwakheden van simpele cryptografische methodes.
8. Cryptografische methodes die tegenwoordig toegepast worden, met bijbehorende voor- en nadelen.
9. Bepalen welke security doelen met een bepaald protocol behaald worden en welke niet.
10. De klassen van aanvallen op protocollen en het voorkomen van deze aanvallen.
11. Hoe symmetrische cryptografie wordt gebruikt bij het e-passport en wat de zwakheden zijn.
12. Methodes voor het vercijferen en ontcijferen van streams.

Hashes

13. Wat een hashfunctie is en wat bijbehorende eigenschappen zijn.
14. De gevallen waarin het wel of niet verstandig of nodig is een hashfunctie te gebruiken (en waarom).
15. Het gebruik van hashes in toepassingen als RIES en kilometerheffing en de problemen die dat oplevert.

Asymmetric crypto

16. De werking van asymmetrische cryptografie (inclusief notatie).
17. Het vercijferen en ontcijferen van teksten met RSA.
18. De getaltheorie die nodig is om RSA te kunnen toepassen.
19. Het behalen van security doelen met asymmetrische cryptografie.
20. Digitale handtekeningen en blinde digitale handtekeningen met de praktijksituaties waarin ze toegepast worden.
21. Manieren om publieke sleutels veilig te verspreiden m.b.v. certificaten en de voor- en nadelen van die manieren.
22. Het discrete logprobleem en het toepassen daarvan: Diffie-Hellman en El Gamal.

    Applications

23. Het verschil tussen authenticatie in de echte en digitale wereld.
24. De voor- en nadelen van wachtwoorden en biometrie.
25. De werking van identiteitsmanagement via sleuteldistributiecentra m.b.v. tickets en hoe dit wordt toegepast.
26. Wat acces control is en voor welke security doelen (op welke manieren) het gebruikt kan worden.
27. De protocollen die er zijn voor netwerkbeveiliging en wat mogelijke aanvallen op die protocollen zijn.

In het algemeen valt op dat de theorie vaak kort en bondig besproken wordt, waarna wordt ingegaan op voorbeelden en toepassingen uit de praktijk. Soms ontbreken er aspecten in die korte uitleg die van te voren gegeven wordt. Deze aspecten worden dan uitgelegd aan de hand van de voorbeelden en toepassingen. De onderwerpen komen achter elkaar aan bod, waardoor de uitleg vaak bottum-up gegeven wordt. Al biedt de inhoudsopgave van de slides wel een algemene structuur.

5.1.3 Vergelijking onderwerpen collegeslides en leerdoelen

De leerdoelen, zoals die in de studiegids (*Studiegids Security*, 2011) geformuleerd zijn, zijn veel algemener dan de onderwerpen die in de collegeslides (Jacobs, 2011c) aan bod komen.

Het eerste leerdoel komt het meest letterlijk terug in het eerste onderwerp. Daarnaast worden ook veel toepassingen behandeld in de collegeslides, waarmee getoond wordt welke aspecten van security een rol spelen te herkennen zijn in die toepassing.

Het tweede leerdoel vraagt om het herkennen van de security doelen. De security doelen zijn het tweede onderwerp in de lijst. Verder worden komen de security doelen aan bod in het negende, negentiende en het zesentwintigste onderwerp. Bij deze drie onderwerpen wordt inderdaad gevraagd om het herkennen van de doelen in een bepaald deelgebieden van de security, namelijk protocollen, asymmetrische cryptografie en access control.

Het derde leerdoel stelt dat de student in staat moet zijn om technieken, waarmee security doelen te behalen zijn, te beschrijven, evalueren en te bedenken. De drie bovengenoemde onderwerpen voldoen hier weer aan, maar eigenlijk kun je bijna alle technieken die aan bod komen wel indelen bij één of meer security doelen, deze technieken zorgen er allemaal voor dat er een vorm van beveiliging tot stand komt.

Het vierde doel beoogt dat de student de gevolgen van securitytechnologieën kan inschatten. De toepassingen die behandeld worden in de collegeslides tonen de gevolgen van zo'n toepassing. De student moet dus zelf een stap verder kunnen gaan dan de collegeslides en deze gevolgen ook kunnen inschatten voor nieuwe situaties.

De geïnventariseerde onderwerpen zijn dus veel specifieker dan de leerdoelen en vormen meer een middel dan een eindpunt op zichzelf om deze leerdoelen te halen. Het is zeker mogelijk dat een andere lijst van onderwerpen ook aansluit op de leerdoelen. Deze lijst sluit zeker aan op de beoogde leerdoelen.

5.1.4 Vergelijking onderwerpen collegeslides en assignments

Bij het vak Security worden niet alleen colleges met collegeslides (Jacobs, 2011c) gegeven, de studenten moeten ook zelf aan de slag met opdrachten (Jacobs, 2011b), zoals al bleek uit de studiegids (*Studiegids Security*, 2011). De opdrachten, die gegroepeerd zijn in assignments, moeten natuurlijk wel aansluiten op de onderwerpen die in de collegeslides behandeld worden. De mate van overeenkomst zal daarom besproken worden.

Hieronder staat een tabel met voor iedere assignment de onderwerpen die daarin voorkomen. Het cijfer in een cel (die bij een onderwerp en assignment hoort) is het nummer van de opdracht van die assignment waar het onderwerp aan bod komt.

		Assignments											
		1	2	3	4	5	6	7	8	9	10	11	12
Onderwerpen	1	1											
	2	2											
	3			2,3,4	1	2	1,3						
	4			2,3,4	1	2	1,3						
	5	3,4,5	2,3										
	6	3,4,5	2,3		2		4						
	7	3,4,5	1,2				2						
	8												
	9			1									
	10			3,4	1	2							
	11			4									
	12				3								
	13					1,2	3						
	14					2	1						
	15												
	16								4				
	17								2,3,4				
	18							1,2,3,4		1			
	19								1				
	20									1			
	21											1	
	22										1,2	2	
	23												
	24												
	25											3	
	26												
	27									2			1,2,3

Tabel 2: Onderwerpen per assignment

Wat opvalt is dat een paar onderwerpen van de collegeslides helemaal niet aan bod komen in de assignments. Andersom blijken er geen opdrachten te zijn die niet over minstens één onderwerp uit de collegeslides gingen. De onderwerpen die ontbreken in de assignments zijn onderwerp 8, 15, 23, 24 en 26. Onderwerp 8 gaat over de huidige toepassingen van cryptografische technieken. De cryptografische technieken komen wel aan bod in de assignments, dus misschien waren deze toepassingen hoofdzakelijk bedoeld om de theorie te verduidelijken en te laten zien hoe de technieken

in de praktijk kunnen worden toegepast, of komen er andere toepassingen aan bod in de assignments. Voor onderwerp 15 geldt hetzelfde, alleen gaat het dan over hashes. Over onderwerp 23, het verschil tussen authenticatie in de echte en digitale wereld is nog wel een opdracht te bedenken, bijvoorbeeld waarbij je gevraagd wordt het verschil voor een specifiek geval te beschrijven. Al was dit wel een onderwerp wat maar kort aan bod komt en bovendien als inleiding dient op de andere onderwerpen, waardoor het misschien minder van belang was om dit specifieke onderwerp terug te laten komen in de assignments.Onderwerp 24 gaat weer over toepassingen, namelijk wachtwoorden en biometrie, dus voor dit onderwerp geldt hetzelfde als de onderwerpen 8 en 15. Het is ook wel mogelijk om over onderwerp 26 een opdracht te bedenken. Bovendien is het opvallend dat er in de leerdoelen zoveel nadruk wordt gelegd op het herkennen en toepassen van de security doelen. Een mogelijke verklaring dat het onderwerp niet aan bod is gekomen is dat het als een van de laatste onderwerpen aan bod kwam in de collegeslides waardoor er geen ruimte meer was in de laatste assignments om hierover een opdracht toe te voegen. Behalve onderwerp 26 ontbreekt er dus niet echt iets structureels uit de collegeslides in de assignments.

Verder is te zien dat de onderwerpen 3 en 4, wat zijn (veilige) protocollen, wel in 4 assignments aan bod komen. Dit lijkt te impliceren dat protocollen en hun veiligheid een erg belangrijk onderwerp is in de security. Verder valt op dat de onderwerpen 5,6 en 7, over symmetrische cryptografie, in de eerste twee assignments staan, terwijl protocollen eerder dan symmetrische cryptografie aan bod komen in de collegeslides. Een mogelijke verklaring hiervoor is dat protocollen pas echt interessant worden als je cryptografie gebruikt en dat er relatief weinig kennis nodig is om een opdracht over symmetrische cryptografie te kunnen maken, iedereen heeft wel eens geheimschrift gebruikt. De andere onderwerpen komen netjes op de volgorde aan bod in de assignments zoals ze in de collegeslides aan bod kwamen.

De meeste opdrachten gaan over één of twee onderwerpen. Maar bijvoorbeeld opdracht 2 van assignment 5 gaat wel over 5 onderwerpen. Dit lijkt misschien veel, maar dat valt wel mee als je naar de inhoud van de onderwerpen kijkt. De onderwerpen 3,4 en 10 gaan over protocollen. De onderwerpen 13 en 14 over hashfuncties. Deze opdracht gaat dan ook over een protocol waarin hashes gebruikt worden. Dit is een logische combinatie, waar ook uitgebreide toepassingen voor zijn volgens onderwerp 15. De combinatie van de onderwerpen 3,4 en 10 (protocollen) komt ook al voor in opdracht 4 van assignment 3, maar dan nog met onderwerp 11 erbij: toepassingen van symmetrische cryptografie. Dit vormt een zelfde soort combinatie als voor de vorige rij onderwerpen: deze opdracht gaat over een protocol van een toepassing van symmetrische cryptografie. De laatste combinatie van onderwerpen die opvalt is die van de onderwerpen 5,6 en 7. Deze drie komen aan bod in opdracht 3,4 en 5 van assignment 1. De drie onderwerpen gaan over symmetrische cryptografie, dus passen ze prima bij elkaar.

5.1.5 Bloom categorieën van tentamenvragen

In onderstaande tabel wordt van elke vraag van het tentamen (Jacobs, 2011a) aangegeven bij welke categorie van Blooms taxonomie die vraag hoort. In *Appendix* is het tentamen bijgevoegd. Te zien is dat vooral de categorieën van hogere niveaus getest worden, waardoor de leerlingen die het tentamen maken ook op een redelijk hoog niveau getoetst worden.

Vraag	Categorie
1(a)	Toepassing
1(b)	Evaluatie
1(c)	Toepassing
1(d)	Evaluatie
2(a)	Toepassing
2(b)	Toepassing
3(a)	Toepassing
3(b)	Toepassing
3(c)	Toepassing
3(d)	Kennis, Toepassing
3(e)	Toepassing
4(a)	Analyse, Synthese
4(b)	Analyse, Synthese
4(c)	Analyse, Synthese
4(d)	Toepassing

Tabel 3: Bloom categorieën per tentamenvraag

5.2 Enigma

Enigma is een lesmethode waarmee een volledig lesprogramma van het middelbare schoolvak Informatica (havo en vwo) gevuld kan worden. Enigma is geen boek, maar een website waarop alle materialen beschikbaar worden gesteld. Op deze website (Enigma, 2013) wordt uitgelegd hoe de methode in elkaar zit. Het is opgedeeld in een aantal onderdelen. Ten eerste is er het *Kernprogramma*, bedoeld voor in de vierde klas. Ten tweede is er een *Verdiepingsprogramma*, bestemd voor 5vwo. Ten slotte is er een *Examenprogramma* voor de examenklassen. Daarnaast zijn er nog extra modules beschikbaar. Al die onderdelen bevatten modules over specifieke onderwerpen.

Een van die modules is de module Cryptografie. Deze module is onderdeel van het *Verdiepingsprogramma*. Omdat cryptografie onderdeel is van security, zal deze geanalyseerd worden. De module Cryptografie stelt een *Informatieboek* en *Verwerkingsboek* en een *Toets* beschikbaar. Daarnaast is er ook een *Interactieve module*, een website die het *Informatieboek*, *Verwerkingsboek* kan vervangen. Veel van de uitleg wordt beschikbaar gesteld in filmpjes. Bij de opdrachten krijg je gelijk te zien of je het goed hebt bij een meerkeuzevraag of een antwoord als je op een knop klikt bij een open vraag. Verder is er nog een website, *e-Wish*, die de leerling kan gebruiken bij het maken van de opdrachten uit het *Verwerkingsboek*, maar gebruik daarvan is niet noodzakelijk. De *Interactieve module* en de combinatie *Informatieboek* en *Verwerkingsboek* verzorgen dus hetzelfde onderwijs op een andere manier. Omdat de module (security) net als het *Informatieboek*, het *Verwerkingsboek* en de *Toets* met tekst werkt, zijn voor de analyse alleen deze bronnen in beschouwing genomen.

5.2.1 Inventarisatie van onderwerpen

Hieronder is de opbouw van het *Informatieboek* in hoofdstukken en paragrafen weergegeven. De onderwerpen die er aan bod komen staan voor elk deel eronder vermeld.

1. Inleiding
   a. Wat cryptografie is
   b. Opbouw van de module
   c. Redenen voor gebruik van cryptografie
   d. Ontwikkeling van cryptografie
2. Cryptografie tot de 20^e eeuw

2.1 Grieken en Perzen
   a. Geschiedenis over eerste geheime bericht
   b. Stenografie
   c. Skytale

2.2 Caesar
   a. Substitutie
   b. Transpositie
   c. Caesar-versleuteling
   d. Algemene begrippen voor een cryptografische methode: encryptie/versleuteling, klare tekst, cijfertekst, decryptie

2.3 Modulorekenen
   a. Modulorekenen
   b. Een uitgebreide Caesar-versleuteling
   c. Monoalfabetische substitutie

2.4 De Viginère
   a. Polyalfabetische substitutie
   b. Alberti-techniek
   c. De cryptografische methode van De Viginère

2.5 Frequentieanalyse
   a. Frequentieanalyse
   b. (Geschiedenis van) cryptoanalyse
   c. Brute force attack
   d. Letterfrequentie
   e. Herhaling van woordpatronen

3. Cryptografie vanaf de 20^e eeuw

3.1 Het Zimmermann telegram
   a. Het belang van cryptografie voor militairen
   b. De geschiedenis rond het Zimmermann telegram

3.2 De Enigma-machine
   a. De onderdelen/opbouw van de Enigma-machine
   b. Het kraken van de Enigma-machine

4. Digitale cryptografie

4.1 XOR-versleuteling
   a. Hoe XOR-versleuteling werkt

4.2 Symmetrisch en asymmetrisch
   a. Symmetrie (van de sleutel)
   b. Asymmetrie (van de sleutels)
   c. Asymmetrische versleuteling (met koffertjes)

4.3 Public en private key
   a. public key en private key
   b. Wat een geschikte functies is voor asymmetrische versleuteling
   c. $Y^X \mod P$ als versleutelmethode
   d. Het Diffie-Hellman-systeem

4.4 De kracht van RSA
   a. Het ontstaan van RSA
   b. De werking van RSA
   c. De voordelen van RSA
   d. Priemfactorontbinding en de moeilijkheid daarvan

4.5 Blokversleuteling
   a. Blokversleuteling

4.6 De Man-in-the-middle attack
   a. Main-in-the-middle attack
   b. Hashfunctie
   c. MD5

4.7 Pretty good privacy
   a. De ontwikkeling van security (in de laatste jaren)
   b. Hoe PGP werkt
   c. Gevolgen voor de uitvinder van PGP (Zimmermann)

5.2.2 Leerdoelen

Hieronder staat de leerdoelen zoals ze vermeld worden in het Verwerkingsboek:

'Na verwerking van dit hoofdstuk:

1. weet je hoe de cryptografie zich vanaf de oudheid heeft ontwikkeld;
2. weet je wat de basisbegrippen zijn van de cryptografie (zoals klare tekst, sleutel, geheime tekst (cijfertekst), encryptie, versleuteling of vercijfering, decryptie);
3. ken je het verschil tussen symmetrische en asymmetrische encryptie;
4. ken je het verschil tussen een substitutie- en transpositiemethode;
5. weet je wat monoalfabetische en polyalfabetische substitutie is;
6. weet je wat stenografie is;
7. heb je inzicht in symmetrische en asymmetrische versleutelingstechnieken;
8. weet je welke rol frequentieanalyse speelt bij het ontcijferen van geheime berichten;
9. weet je hoe de Enigma-machine werkt;
10. weet je hoe public en private key ingezet worden bij moderne cryptografie;
11. weet je hoe modulorekenen toegepast wordt bij moderne cryptografie;
12. ken je het belang van authenticatie;
13. begrijp je waarom blokversleuteling toegepast wordt;
14. weet je hoe RSA en PGP werkt en waarom een hashfunctie belangrijk is.'

Wat opvalt is dat veel leerdoelen met *weet je* beginnen, wat aangeeft dat alleen om *Kennis* wordt gevraagd, de laagste categorie van Blooms taxonomie. De inhoud van de hele zin van die leerdoelen bevestigt dit beeld. Ook leerdoel 12 gaat alleen over *Kennis*. Leerdoel 3 en 4 vragen om het kunnen geven van een verschil, wat typerend is voor de categorie *Inzicht*. Ook leerdoel 7 hoort bij de categorie *Inzicht*, er wordt hier immers om inzicht gevraagd. Verder is het woord *begrijp* van leerdoel 13 ook kenmerkend voor de categorie *Inzicht*. De leerdoelen vragen dus maar om een laag niveau van leren. De vier categorieën boven *Inzicht* komen helemaal niet aan bod.

5.2.3 Vergelijkingstabel leerdoelen en onderwerpen

In onderstaande tabel is voor elk leerdoel aangegeven welke onderwerpen onder dit leerdoel vallen. Als het onduidelijk was of een onderwerp bij een leerdoel hoorde of niet, is in de tekst over dit onderwerp gekeken om een keuze te kunnen maken. Er is geprobeerd om alleen de onderwerpen die noodzakelijk zijn voor het leerdoel met een x aan te geven. Er kunnen best meer onderwerpen zijn die minder direct onder een leerdoel vallen. Maar als die ook aangegeven zouden worden is het moeilijker om de grens te trekken tussen de onderwerpen die wel en niet bij een leerdoel horen. Ook krijg je dan een minder scherp beeld. De onderwerpen komen uit een module over één afgebakend onderwerp, namelijk cryptografie, dus het ligt voor de hand dat er dingen zijn die samenhangen.

		Leerdoelen													
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
	1a	x	x												
	1b	x													
	1c	x													
	1d	x													
	2.1a	x													
	2.1b						x								
	2.1c														
	2.2a				x										
	2.2b				x										
	2.2c				x										
	2.2d		x												
	2.3a											x			
	2.3b				x										
	2.3c					x									
	2.4a					x									
	2.4b														
	2.4c				x										
	2.5a								x						
	2.5b	x							x						
	2.5c														
	2.5d								x						
	2.5e								x						
Onderwerpen	3.1a	x													
	3.1b	x													
	3.2a									x					
	3.2b	x													
	4.1a														
	4.2a			x				x							
	4.2b			x				x			x				
	4.2c			x				x			x				
	4.3a							x			x				
	4.3b	x						x				x			
	4.3c							x				x			
	4.3d							x				x			
	4.4a	x													
	4.4b							x				x			x
	4.4c	x											x		
	4.4d														
	4.5a													x	
	4.6a														x
	4.6b														x
	4.6c														
	4.7a	x													
	4.7b														x
	4.7c	x													

Tabel 4: Onderwerpen per leerdoel

5.2.4 Onderwerpen per leerdoel

Alle leerdoelen hebben onderwerpen die verspreid zijn over hooguit 3 paragrafen, behalve leerdoel 1. Dit komt omdat leerdoel 1 heel algemeen is, je kan bijna alles wel onder ontwikkeling laten vallen. In de tabel zijn alleen de onderwerpen aangegeven die beschrijven hoe die ontwikkeling gegaan is, de methodes om geheime berichten te maken zijn weggelaten, ook al zijn dit vaak de uitkomsten van een bepaalde ontwikkeling. Dit is gedaan om niet bijna alle onderwerpen onder leerdoel 1 te laten vallen, waardoor er niet meer zoveel over te zeggen valt. Ook horen veel van de onderwerpen die misschien wel onder leerdoel 1 zouden kunnen vallen, al bij een ander leerdoel.

Het aantal onderwerpen dat onder één leerdoel valt, loopt uiteen per leerdoel. Een mogelijke verklaring hiervoor is dat sommige leerdoelen veel specifieker zijn en andere veel algemener. Leerdoel 7 is bijvoorbeeld best algemeen door te vragen naar inzicht over symmetrische en asymmetrische versleutelingstechnieken. Je moet over heel wat onderwerpen iets weten om hier echt wat over te kunnen zeggen. Daarentegen is leerdoel 6 heel specifiek, er wordt alleen gevraagd om kennis over één specifieke versleutelingstechniek, namelijk stenografie.

5.2.5 Leerdoelen per onderwerp

De meeste onderwerpen, 28 van de 45 onderwerpen, vallen onder één leerdoel. Dit is een goede indicatie dat de leerdoelen de onderwerpen die aan bod komen goed dekken en dat de leerdoelen elkaar niet te veel overlappen. Maar er zijn wel paar onderwerpen die bij een ander aantal leerdoelen horen.

Er zijn vier onderwerpen die bij drie leerdoelen horen: 4.2b, 4.2c, 4.3b en 4.4b. Drie is het hoogste aantal leerdoelen per onderwerp van alle geïnventariseerde onderwerpen. Alle vier de genoemde onderwerpen gaan over asymmetrische versleuteling: 4.2b en 4.2c leggen uit wat asymmetrische versleuteling is, 4.3b legt uit wat er nodig is om asymmetrische versleuteling mogelijk te maken en 4.4b is een realisatie van asymmetrische versleuteling. Dat al deze onderwerpen over asymmetrische versleuteling gaan is een indicatie dat de schrijvers van deze module dit concept erg belangrijk vonden.

Er zijn zeven onderwerpen die bij twee leerdoelen horen: 1a, 2.5b, 4.2a, 4.3a, 4.3c, 4.3d en 4.4c. De onderwerpen 4.3a, 4.3c, 4.3d en 4.4c gaan allen over asymmetrische versleuteling, wat nog eens bevestigd dat dit concept belangrijk wordt gevonden. Onderwerp 4.2a past eigenlijk ook bij voorgenoemde groep, want door symmetrie uit te leggen wordt duidelijker wat asymmetrie is. Bovendien is symmetrie een erg algemeen concept waardoor het niet erg opvallend is dat dit onderwerp onder twee leerdoelen valt. Onderwerp 2.5b bevat eigenlijk twee deelonderwerpen: cryptoanalyse en de geschiedenis daarvan. Maar omdat die twee samen en door elkaar heen worden uitgelegd zijn ze moeilijk te scheiden. Onderwerp 1a, wat cryptografie is, moet de leerling kennen, omdat dit is waar het hoofdstuk over gaat. Dit onderwerp is het nodig om algemene onderwerpen als de ontwikkeling van de cryptografie en basisbegrippen van de cryptografie te kunnen begrijpen.

Er zijn zes onderwerpen die bij geen enkel leerdoel passen: 2.1c, 2.4b, 2.5c, 4.1a, 4.4d en 4.6c. In het algemeen valt aan deze onderwerpen op dat ze heel specifiek zijn en/of een opstapje vormen naar andere onderwerpen. Hierdoor is het begrijpelijk dat deze onderwerpen niet onder de leerdoelen vallen, omdat leerdoelen in het algemeen vaak abstracter en algemener zijn en dus alleen de belangrijkste zaken verwoorden. Onderwerp 2.1c, de skytale, is een specifiek voorbeeld. Al is het wel opvallend dat er voor onderwerp 2.1b, stenografie, wel een leerdoel is, want dit zijn allebei methodes uit de tijd van de Grieken en Perzen om geheime berichten te maken. Misschien komt dit doordat stenografie makkelijk op papier te gebruiken is, terwijl je voor de skytale zo'n stok nodig hebt, wat minder praktisch is voor het onderwijs over dit onderwerp. Onderwerp 2.4b, de Alberti-techniek, is een opstapje naar het onderwerp waar de paragraaf ook naar genoemd is: De Vigenère. Onderwerp 2.5c, brute force attack, is een specifiek onderwerp waarvan de tekst twee ervoor genoemde onderwerpen aan elkaar koppelt. Onderwerp 4.1a, XOR-versleuteling, is erg specifiek, en vormt ook een opstapje naar versleuteling in het digitale tijdperk, zoals ook wordt aangegeven in de tekst, waardoor het onderwerp niet zo belangrijk is, maar wel een hulp kan zijn om de overstap naar dit nieuwe hoofdstuk makkelijker te maken. Onderwerp 4.4d over

priemfactorontbinding vormt een extra toelichting op en argumentatie voor het gebruik van RSA. RSA zelf is goed te snappen zonder iets over priemfactorontbinding te weten. Onderwerp 4.6c is een specifiek voorbeeld van een hashfunctie, het onderwerp dat daarvoor is uitgelegd. Misschien is dit onderwerp dus meer als illustratie bedoeld dan als iets wat de leerling echt moet weten.

5.2.6 Vergelijking leerdoelen en opdrachten

In het *Verwerkingsboek* staan voor elke hoofdstuk van het *Informatieboek* een aantal opdrachten. Voor iedere opdracht is vastgesteld welke leerdoelen ermee getoetst worden. Daarbij is bepaald bij welke categorie van leren (van Blooms taxonomie) de opdracht past. Voor elk opdrachtnummer wordt het hoofdstuknummer vermeld met een : ertussen.

Opdrachten	Categorie(ën)	Leerdoelen													
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
1:1	Kennis	x	x												
1:2	Kennis, Inzicht	x													
2:3	Kennis	x													
2:4	Kennis, Inzicht						x								
2:5	Inzicht				x			x							
2:6	Toepassing		x		x			x							
2:7	Toepassing				x			x							
2:8	Toepassing											x			
2:9	Kennis		x		x	x		x							
2:10	Inzicht					x		x							
2:11	Inzicht							x							
2:12	Inzicht							x							
2:13	Inzicht							x							
2:14	Inzicht							x							
2:15	Kennis								x						
2:16	Inzicht								x						
2:17	Kennis	x													
2:18	Kennis, Inzicht		x		x	x		x							
2:19	Kennis	x													
2:20	Kennis	x													
2:21	Kennis	x													
2:22	Toepassing							x							
2:23	Synthese						x								
2:24	Toepassing				x			x				x			
2:25	Toepassing				x			x				x			
2:26	Toepassing				x	x		x							
2:27	Inzicht		x					x							
2:28	Kennis, Inzicht		x					x							
2:29	Toepassing								x						
2:30	Toepassing							x							
2:31	Evaluatie				x	x		x							
2:32	Toepassing				x			x							
3:33	Kennis	x													
3:34	Kennis	x													
3:35	Kennis	x													
3:36	Inzicht	x													

Tabel 5: Leerdoelen en Bloom categorieën per opdracht (1)

Opdrachten	Categorie(ën)	Leerdoelen													
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
3:37	Kennis	x													
3:38	Toepassing									x					
3:39	Kennis									x					
3:40	Kennis	x													
3:41	Kennis	x													
4:42	Kennis							x							
4:43	Kennis, Toepassing			x				x							
4:44	Kennis		x					x			x				
4:45	Kennis, Inzicht							x			x				
4:46	Kennis										x				
4:47	Kennis, Inzicht	x						x							
4:48	Kennis	x													
4:49	Kennis											x			
4:50	Kennis							x							
4:51	Kennis	x						x							
4:52	Kennis														x
4:53	Kennis, Toepassing												x		
4:54	Kennis														x
4:55	Kennis														x
4:56	Kennis														x
4:57	Kennis													x	
4:58	Kennis														x
4:59	Kennis, Inzicht													x	x
4:60	Kennis	x													
4:61	Kennis	x													
4:62	Kennis	x													x
4:63	Kennis														x
4:64	Toepassing							x							
4:65	Toepassing											x			
4:66	Toepassing											x			
4:67	Kennis											x			
4:68	Toepassing														x
4:69	Toepassing														x
4:70	Kennis, Toepassing			x	x			x							
4:71	Toepassing							x							
4:72	Toepassing														x
4:73	Kennis														x
4:74	Kennis														x
4:75	Kennis, Inzicht														x

Tabel 6: Leerdoelen en Bloom categorieën per opdracht (2)

Uit bovenstaande tabel blijkt dat de leerdoelen op hoger niveau getoetst worden dan dat de formulering van die leerdoelen aangeeft. *Toepassing* wordt redelijk vaak getoetst, terwijl geen van de leerdoelen in deze categorie valt. Er is één opdracht die *Synthese* toetst en één die *Evaluatie* toetst, dat is wel wat weinig voor 75 opdrachten. *Analyse* komt helemaal niet voor.

Alle leerdoelen aan bod. De leerdoelen 1,7 en 14 komen erg veel aan bod. Een verklaring hiervoor is dat leerdoel 1 en 7 erg algemeen zijn, waardoor veel opdrachten daar op een of andere manier bij aansluiten. Bovendien was het soms nodig leerdoel 7 te kiezen als er geen specifieker leerdoel was, bijvoorbeeld als het over XOR-versleuteling ging. Leerdoel 14 noemt 3 onderwerpen,

waarvan RSA een erg uitgebreid onderwerp is.

De leerdoelen 3 en 12 komen maar één keer voor. De formulering *ken je het verschil* en de gelijkenis met leerdoel 7 maakte dat dit leerdoel niet zo goed paste of dat leerdoel 7 veel beter paste bij de opdracht. Leerdoel 12 gaat over een onderwerp dat maar heel kort behandeld wordt in de tekst van het Informatieboek. Dat er dan ook niet veel opdrachten over authenticatie gaan is dan wel logisch.

5.2.7 Bloom categorieën van toetsvragen

Met de opdrachten wordt de leerling getoetst op wat hij geleerd heeft, maar vaak is de (eind)toets bepalend voor de beoordeling van de leerling voor het vak. Hieronder is weergegeven welke categorieën van Blooms taxonomie aan bod komen bij de vragen in de *Toets*. Omdat de modules van Enigma vertrouwelijk zijn kan de *Toets* niet bijgevoegd worden, zoals bij *Het vak Security* wel is gedaan. Om toch een beeld te geven waar de vraag over gaat, wordt per vraag aangegeven welke leerdoelen er getoetst worden.

Vraag	Categorie	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	Kennis		x	x											
2	Kennis	x	x					x							
3	Synthese		x					x							
4	Kennis				x										
5	Kennis		x												
6	Kennis											x			
7	Toepassing							x							
8	Kennis					x									
9	Toepassing					x		x							
10	Kennis				x	x		x							
11	Kennis								x						
12	Inzicht							x							
13	Kennis	x								x					
14	Kennis	x								x					
15	Toepassing			x				x							
16	Kennis										x				
17	Kennis														x
18	Kennis														x
19	Kennis												x		
20	Inzicht							x							
21	Kennis													x	x

Tabel 7: Bloom categorieën per toetsvraag

De *Toets* bevat dus veel vragen die *Kennis* toetsen en relatief weinig vragen die andere categorieën toetsen. Dit komt wel veel meer overeen met de categorieën van de leerdoelen, maar geeft een indicatie dat de opdrachten uit het *Verwerkingsboek* moeilijker zijn dan dan wat een leerling eigenlijk zou moeten aankunnen.

Bij het bepalen van de leerdoelen per toetsvraag viel op dat er enkele vragen bijna letterlijk overeen kwamen met een leerdoel. Dit draagt erin bij dat de categorieën van de *Toets* en de leerdoelen zo overeen komen. Leerdoel 6, over stenografie, komt niet voor in de toets, al is het wel mogelijk dat de leerling die de toets maakt stenografie noemt als voorbeeld bij een meer algemene vraag. Net zoals bij de opdrachten komt leerdoel 7 vaak naar voren in de toetsvragen, omdat dit zo'n algemeen leerdoel is. De leerdoelen 1 en 14, die in de opdrachten vaak aan bod kwamen, komen in de toetsvragen niet bijzonder vaak voor in vergelijking met de aantallen van de andere leerdoelen. Omdat er maar 21 vragen gesteld worden en er 14 leerdoelen zijn, is het niet opvallend dat een aantal leerdoelen maar één keer aan bod komen.

5.3 Interview met docent

Hieronder staan de resultaten van het interview met een ervaren docent op de Radboud Universiteit Nijmegen. Het uitgeschreven interview staat in de *Appendix*. Hieronder wordt het interview weergegeven per vraag zoals beschreven is in de *Methode*. Bij elke vraag wordt eerst weergegeven wat er gezegd is. Deze tekst komt overeen met die in de appendix, al zijn op enkele plaatsen de zinnen aangepast om ze goed te laten lopen. Vervolgens wordt een samenvatting gegeven van wat gezegd is, waardoor een samenhangend antwoord op de vraag gegeven wordt.

1. Wat wilt u dat studenten leren over dit idee?
   Bij Hardware security en Software security komt het volgende aan bod:

   - Standaard manieren om security eisen te inventariseren.
   - Standaard manieren om security eisen te garanderen.
   - Technieken die je kunt gebruiken ter beveiliging.
   - Wat er typisch mis gaat.
   - Creatief nadenken.
   - Het beschrijven van standaard dingen die fout kunnen gaan in software, want er zijn een heleboel klassieke fouten: bufferoverflows, sql-injection, cross-site scripting.
   - De ervaring van het bouwen van een hardware-oplossing.
   - Weten welke standaard fouten er zijn: dit moet je niet doen, want dan gaat het daar mis. En dat, als studenten later applicaties gaan bouwen in de praktijk, in een bepaalde programmeertaal, ze ook actief opzoek gaan naar kennis over die standaard fouten in die specifieke programmeertaal.
   - Meer algemeen, wil je een bepaalde security mindset meegeven, namelijk dat je kritisch nadenkt over een ontwerp en daar probeert gaten in te schieten. Je wilt dat mensen naar hun applicatie kijken als een aanvaller: wat zijn nou de dingen die ik zou willen aanvallen, hoe zou ik dat doen? Zo denk je na of je op de goede plekken dingen goed beveiligd hebt.
   - Je leert dat het een moeilijk is om een webapplicatie te begrijpen. Je moet uitzoeken hoe het georganiseerd is en waar er wel en niet nagedacht is over de security.

   De onderwerpen die aan bod komen zijn dus: eisen, beveiligingstechnieken en standaard fouten. Het is de bedoeling dat de student door kennis over deze onderwerpen een beter beveiligd systeem kan bouwen en kan onderzoeken of een bestaand systeem goed beveiligd is.

   Verder wordt beoogd om de student een security mindset mee te geven, hem of haar te laten ervaren hoe moeilijk het is om een veilig systeem te bouwen en om creatief nadenken bij studenten te stimuleren.

2. Waarom is het belangrijk dat studenten dit leren?

   Eisen Het is belangrijk dat de studenten de eisen leren. Als mensen een systeem bouwen kijken ze in eerste instantie naar de functionaliteit en dan gaan ze hooguit achteraf pas nadenken over wat er allemaal mis kan gaan. Ik denk dat het belangrijk is dat als je het systeem neerzet, je dan al nadenkt over wat de risico's zijn die je loopt.

   Ervaring Als je mensen zelf een hardware-oplossing laat ontwerpen en implementeren, dan ervaren mensen van hoe lastig dat is en hoe makkelijk het is om daarmee fouten te maken.

   Kennis over de eisen helpt dus om van te voren na te denken over de beveiliging van een systeem, waardoor het makkelijker wordt om in één keer een goed systeem te bouwen. Ervaring met het beveiligen van systemen helpt om het belang van dat beveiligen in te zien.

3. Wat weet u nog meer over dit idee wat de studenten niet hoeven te leren?

   Voorbeelden Alle belangrijke issues wil je wel aan bod laten komen, alle brede thema's komen aan bod. Je kunt altijd meer voorbeelden of meer case-studies geven waarvan je dan toevallig meer weet, maar die kun je niet allemaal behandelen.

   Programmeertalen De standaard fouten komen aan bod, maar ik ga niet voor tien programmeertalen uitleggen hoe je een veilige sql-query maakt waardoor sql-injecten niet mogelijk is.

   De brede thema's komen aan bod, maar er is beperkt ruimte om voorbeelden en case-studies te behandelen en er kan niet ingegaan worden op hoe standaard fouten eruit zien in specifieke programmeertalen.

4. Welke problemen en beperkingen van studenten beïnvloeden uw onderwijs?

   Eisen Bij het bouwen van een oplossing (zie *Hardware-oplossing bouwen* bij vraag 7) zie je dat mensen dingen over het hoofd zien bij het inventariseren van de security eisen. Iets klassieks wat je daar heel vaak ziet is dat iedereen er aan denkt om dingen te versleutelen maar bijvoorbeeld niet om een handtekening erop te zetten of een mac om de integriteit te waarborgen mee te geven. Dat is heel deterministisch dat mensen dat vergeten. We hebben dan bijvoorbeeld tien groepen die je een oplossing laat maken en dan vergeten er zes dat integriteit eigenlijk veel belangrijker is dan confidentialiteit.

   Protocollen In principe is het een protocolprobleem als je integriteit vergeet te checken. Er zijn andere standaard protocolfouten van dat je nonces moet gebruiken om replay-attacks te voorkomen. Moet je ook even aan denken.

   Veel studenten denken er niet aan om integriteit te waarborgen, omdat ze niet verder denken dan het versleutelen, en daarmee confidentialiteit.

5. Welke manieren van denken van de studenten beïnvloeden uw onderwijs?

   Hardware-oplossing bouwen De eerste reflex van mensen is om dingen te gaan versleutelen terwijl dat eigenlijk helemaal niet belangrijk is. Dus daar zie je wel patronen in. Dat zie je wel bij security, dat mensen steeds dezelfde fouten maken. Dat heeft een voordeel, dan kun je er wat aan doen. Als iedereen de hele tijd iets anders fout doet, dan kun je er niks aan doen. Aan de andere kant is het frustrerend, dat moet je nu toch weten. Maar het zijn natuurlijk telkens nieuwe studenten.

   In de security worden vaak dezelfde fouten gemaakt, zoals het vergeten van integriteit. Het onderwijs kan de studenten helpen deze fouten te voorkomen of te ontdekken.

6. Wat zijn andere factoren die uw onderwijs beïnvloeden?

   Literatuur Soms is er weinig literatuur beschikbaar, of niet echt de geschikte literatuur. Ik probeer om wetenschappelijke publicaties als literatuur aan te voeren, dat is ook leuk als mensen dat eens een keer lezen. Of dat ik zelf stukken dictaat schrijf.

   Smart-card Als je software gaat schrijven voor een smart-card, merk je dat dat een redelijk obscuur en raar platform is om op te programmeren.

   - Je moet heel voorzichtig programmeren, want je hebt heel weinig resources op je systeem, 256 bytes RAM, dat is anders dan de gemiddelde computer.
   - Je moet op heel laag niveau programmeren: met bytes en bits. Dat doe je met normaal programmeren eigenlijk niet want dan trek je een paar van die bibliotheken open en dan ga je aan de slag.

- Met dit soort embedded hardware is het debuggen afgrijselijk lastig. Normaal als je een programma hebt en hij doet het niet dan zet je er een paar print-lines in, maar op een smart-card kan je er geen print-lines in zetten. Als je bijvoorbeeld in Java een nullpointer exception hebt, dan krijg je een nullpointer exception en stack trace en kun je precies zien waar die exception zit. Op zo'n smartcard krijg je: error. Dan moet je zelf uitvogelen wat er dan mis was.
- In zo'n omgeving moet je veel gedisciplineerder programmeren, want je kunt niet gewoon wat programmeren en dan wel zien waar het fout gaat en dan een beetje bijsturen, want dat werkt daar helemaal niet.

Crypto Als je met crypto programmeert, is dat ontzettend lastig om te debuggen, omdat de bedoeling van crypto is dat je helemaal geen informatie lekt. Maar dat betekent met debuggen dat als je een berichtje aan het decrypten bent, maar je hebt een offset net verkeerd, je echt garbage terugkrijgt. En dan kun je bijvoorbeeld ook niet zien dat je een bit te ver bent. Als developer werkt crypto dus tegen je. Als je ergens een key verkeerd hebt geïnstalleerd, krijg je helemaal geen zinnige informatie terug.

Groot Bij de code-review is het probleem dat die applicaties zo verrekte groot zijn. Zo'n smart-card-programmaatje is een paar honderd regels, dat kun je nog een beetje overzien, maar bij een gemiddelde webapplicatie is dat lastiger.

Er is weinig literatuur, maar dit wordt opgelost door wetenschappelijke artikelen te gebruiken of een zelfgeschreven dictaat.

Het programmeren met een smart-card zorgt ervoor dat je heel precies moet programmeren en dat debuggen lastig is. Cryptografie maakt dit debuggen nog lastiger.

Verder is het lastig om webapplicaties te overzien omdat ze zo groot zijn.

7. Wat zijn uw werkwijzen of methodes in uw onderwijs en waarom gebruikt u deze methoden bij het onderwijzen van dit idee?

Creatief nadenken Dat kun je niet echt onderwijzen. Je kunt voorbeelden noemen of anekdotes vertellen, je ziet daar wel terugkerende patronen in van typisch die dingen die mensen fout doen. Maar het blijft lastig. Je kunt niet een checklist maken met tien dingen van 'hier moet je je aan houden en dan gaat het goed'. Uiteindelijk kun je het niet echt onderwijzen. De student moet er zelf achter komen. Al probeer je met de projecten wel te stimuleren dat ze zelf creatief nadenken.

Eisen Je kunt op heel hoog niveau beginnen, confidentialiteit, integriteit, authenticatie, je kan standaard nadenken over wat voor authenticatiemechanismen je gebruikt, hoe je bepaalde verbindingen beveiligd. Het grote probleem bij security is, dat je het maar ergens over het hoofd hoeft te zien en je hangt.

Hardware-oplossing bouwen Bij hardware security laten we de studenten zelf een oplossing bouwen. Ze moeten een systeem ontwerpen, de security eisen formuleren, zelf protocollen maken om het te beveiligen en het uiteindelijk implementeren op een smartcard. Dat is dus vrij constructief.

Code-review Ik laat ik studenten bij Software security een code-review doen voor een webapplicatie. Dus dat ze een webapplicatie moeten bekijken, om te zeggen hoe veilig die is aan de hand van een soort richtlijnen voor zo'n review die zijn gemaakt. Ook om ze even te confronteren met het probleem dat een willekeurige applicatie duizenden regels code heeft.

Vakindeling Wat ik wel altijd probeer is dat mensen zelf ergens mee aan de slag gaan.

Andere opdrachten Software Security Bij software security zitten wel wat opdrachten waarbij ze met tools aan de gang gaan.

Begeleiding De meeste opdrachten worden gewoon thuis gemaakt. Bij sommige opdrachten doen we dan wel eens dat het in een computerzaal is, dat je mensen kan helpen met praktische dingen. Maar dat is niet standaard omdat we met die Kerkhoffs master al onze vakken op één dag schedulen.

Hardware-oplossing bouwen: documentatie Ik gebruik meestal een wiki waar ze dat dan moeten documenteren, omdat ik dan ook meteen feedback of hints kan geven.

Structuur college In een college begin ik meestal met een voorbeeldje, daarna komt algemene theorie. Ik probeer altijd dingen aan voorbeelden op te hangen.

Hardware-oplossing: onderwerp kiezen Bij hardware security hebben we een paar standaard dingen die mensen kunnen implementeren: maak een soort chipknip-achtig iets of een kleine variatie op dat thema. Het komt allemaal op hetzelfde neer.

Software security: onderwerpen kiezen Bij sommige tooltjes dan hebben we gewoon standaard voorbeeldjes, want dan moet je het een beetje gecontroleerd houden, dat je het een beetje voorspelbaar hebt. Maar bij zo'n code-review mogen ze zelf een webapplicatie uitkiezen.

Abstractie Je probeert dingen op verschillende niveaus uit te leggen. Vaak wil je dat mensen de intuïtie achter iets begrijpen. Als je bijvoorbeeld een of andere formelere methode hebt om iets te analyseren, dat mensen snappen hoe zoiets werkt, maar ook dat ze de intuïtie begrijpen van wat je er uiteindelijk mee bereikt. Meestal begin je met voorbeelden om de intuïtie achter het probleem uit te leggen en daarna ga je meer de diepte in. Op het eind probeer je soms nog even terug te koppelen, dus even weer de stap terug te maken, zodat ze weer zien hoe het in het overzicht past.

In de colleges wordt meestal een een nieuw onderwerp begonnen met een voorbeeld. Daarmee wordt de intuïtie achter het probleem uitgelegd. Vervolgens wordt er dieper ingegaan op de details. Soms wordt daarna nog teruggekoppeld naar de intuïtie. Bij onderwerpen als security eisen kan heel abstract begonnen worden.

Naast de college moeten de studenten zelf aan de slag met opdrachten. Als er te veel mogelijkheden zijn liggen de onderwerpen van de opdrachten vast, zo niet, dan mogen de studenten zelf een onderwerp kiezen. De studenten documenteren hun opdrachten op de wiki, waardoor zichtbaar is wat ze doen en ze in de juiste richting gestuurd kunnen worden.

Studenten worden gestimuleerd creatief na te denken door de voorbeelden die gegeven worden en de opdrachten die ze maken.

8. Hoe stelt u vast in welke mate studenten het idee begrepen hebben?

Hardware security Er is geen tentamen. De studenten worden beoordeeld aan de hand van hun Hardware-oplossing en wat kleinere opdrachten die ze met z'n tweeën of individueel doen.

Hardware-oplossing bouwen: presentatie Je laat de studenten iets bouwen en dan moeten ze het verantwoorden en dan geven we daar feedback op. En wij proberen er dan gaten in te schieten. Dat doen we door naar de standaard dingen te kijken die fout kunnen gaan. In het verleden hebben we dan wel gedaan dat ze op het einde een presentatie moeten geven voor de hele groep. Maar soms merk je dan dat we teveel groepen hebben. Als je vijf groepen hebt kun je zeggen van dan vertelt iedereen 10 minuutjes iets. Maar we hebben dit jaar elf groepen, dan wordt het een beetje de vraag of het nog te doen om te laten presenteren, want met zoveel groepjes wordt het vaak ook ontzettend saai. Een alternatief hiervoor is dat je meetings hebt per groepje om even feedback te geven.

Code-review Ze moeten verantwoorden waarop hun conclusie gebaseerd is. Ze hebben een goede conclusie getrokken als ze daar goede argumentatie voor kunnen geven. Je kunt bijvoorbeeld ook kijken of ze de standaard dingen gedaan om een sql-injection etc. te

voorkomen. Als ze dat niet hebben gedaan kun je laten zien dat er daardoor een gat in de beveiliging is. Of je kunt kijken of je een voorbeeld kunt geven waar het mis gaat.

Software security Bij Software security hebben ze drie projecten, twee individueel, de code-review in een groepje en een tentamen op het einde. Het tentamen gaat meer in op de theoretische- of kennisaspecten, niet de praktijkdingen.

Bij Hardware security worden studenten beoordeeld op de opdrachten die ze inleveren en de presentatie die ze over de hardware-oplossing geven. Bij de hardware-oplossing wordt gekeken naar de fouten die gemaakt zijn in de beveiliging.

Bij Software security worden studenten beoordeeld op de opdrachten die ze inleveren en het tentamen. De praktijk wordt getest met de opdrachten, de theoretische aspecten met het tentamen. Bij de code-review-opdracht moet de conclusie ondersteund worden door goede argumentatie. Ook moeten de studenten bij de code-review de standaard fouten hebben onderzocht.

5.4 Visiedocument

Het *Visiedocument* over NLT (Stuurgroep Natuur, Leven en Technologie, 2007) beschrijft hoe het vak NLT vormgegeven zou moeten worden. Het document bevat een aantal aspecten die ook van toepassing zijn op onderwijs over security. Er worden kenmerken gegeven waaraan een NLT-module moet voldoen en er worden een aantal vormen van toetsing voorgesteld.

5.4.1 Kenmerken

Het *Visiedocument* noemt een aantal algemene kenmerken waaraan het onderwijs van NLT moet voldoen. De module security wordt ontwikkeld voor NLT, dus moet er aan deze kenmerken voldaan worden. Per kenmerk zal aangegeven worden wat het kenmerk bijdraagt aan het antwoord op één van de deelvragen. Behalve het vierde kenmerk zijn alle kenmerken een soort richtlijnen die gevolgd moeten worden bij ontwikkeling van een NLT-module.

De eerste drie kenmerken beschrijven specifieke aspecten van de onderwijsaanpak die gebruikt zou moeten worden voor NLT-modules.

Het eerste kenmerk gaat over structuur en flexibiliteit:
'In de lesstof moet een balans zijn tussen een vaste structuur en de mogelijkheid om een eigen richting te gaan bij het doorlopen van een module. De leerling kan hierdoor meer regie krijgen over het eigen leerproces. Het biedt ook de mogelijkheid om bijvoorbeeld gebruik te maken van de expertise of interesse van de docent of om in te gaan op de actualiteit.'
Het centraal stellen van de leerling in zijn of haar leerproces is een kenmerk van het constructivisme, zie het *Theoretisch kader*. Het bovenstaande citaat geeft dus de indruk dat het vanuit NLT belangrijk gevonden wordt dat het onderwijs op een constructieve manier gegeven wordt.

Het tweede kenmerk drukt het belang uit van een activerende didactiek:
'De didactiek die aan de lesstof ten grondslag ligt is voor de leerlingen zo stimulerend en activerend mogelijk. Dit maakt de lesstof voor een leerling aantrekkelijker, waardoor het leerrendement waarschijnlijk hoger zal zijn. Het verwerven van vaardigheden kan alleen als de leerlingen actief deelnemen aan het onderwijsproces.'
De nadruk op het actief deelnemen van de leerling wijst ook weer op een onderwijsaanpak die overeenkomt met het constructivisme, want het constructivisme stelt dat de leerling zelf zich actief moet inzetten om iets te leren.

Het derde kenmerk stelt dat de lNLT-modules uitgaan van de relatie tussen concept en context:
'Door het leggen van logische verbanden tussen concepten, ontstaat een conceptueel netwerk. Een leerling moet leren uit verschillende contexten de onderliggende concepten te abstraheren en te gebruiken.'. Hiervoor wordt een argumentatie gegeven: 'Uitgangspunt is dat door het gebruik van contexten nieuwe kennis makkelijker te verwerven is en ook beter verankerd wordt in het geheugen. Contexten geven een goed beeld van de rol die natuurwetenschap en technologie spelen in de

maatschappij. Door het gebruik van contexten kan makkelijker verwondering worden opgewekt en kan de lesinhoud boeiender en uitdagender zijn.'

Het vierde kenmerk beschrijft waarom ICT goed bij NLT past en dat ICT belangrijk is:
'Informatie en Communicatie Technologie (ICT) kent veel verschijningsvormen, bijvoorbeeld communicatienetwerken, maar ook zeer gevarieerde en complexe informatiesystemen bij bedrijven, overheid, wetenschap en onderwijs.
De rol van ICT in de wetenschap en technologie is zeer groot. Bekende toepassingen zijn het verrichten van metingen ten behoeve van data verzameling, ontwerp en gebruik van modellen voor het doen van voorspellingen (het weer, gedrag van mensen) en het ontwerpen van ingewikkelde systemen als vliegtuigen, auto's en fabrieken en van producten (zowel wat betreft vormgeving als technische uitvoering).'
Bij alle voorbeelden die genoemd worden is wel een security-element aan te wijzen alleen worden ze niet genoemd. Bij communicatienetwerken wil je niet dat iemand zomaar alle communicatie kan afluisteren. Bij veel (complexe) informatiesystemen wil je niet dat iedereen toegang heeft tot vertrouwelijke informatie als bedrijfsgeheimen, informatie over wie wat gestemd heeft, nog niet gepubliceerde stukken en commentaren op leerlingen. Bij dataverzameling moet erop gelet worden dat de privacy niet wordt geschonden en de weermodellen mogen niet zomaar aangepast worden, waardoor verkeerde voorspellingen gedaan worden. Bij het ontwerpen van vliegtuigen, auto's, fabrieken en producten is het ook niet de bedoeling dat iemand zomaar iets aan het systeem veranderd, want dat zou de veiligheid kunnen schaden. Door dit verband geeft het document dus ook een argumentatie waarom security goed bij NLT past en belangrijk is, dus een argumentatie waarom een leerling iets over security zou moeten leren.

Het vijfde en zesde kenmerk gaan over de doelgroep van NLT-modules. De doelgroep is belangrijk, want die bepaalt op welke manier het onderwijs vormgegeven wordt.

Het vijfde kenmerk beargumenteert waarom het lesmateriaal ook geschikt moet zijn voor meisjes: 'De verschillen tussen de profielkeuze bij jongens en meisjes zijn anno 2006 erg groot. Niet alleen kiezen meer jongens dan meisje voor een natuurprofiel, ook wordt door jongens verhoudingsgewijs veel meer voor het NT-profiel gekozen. In het licht van het tekort aan studenten in de natuurwetenschappen en technische vakken is dit zorgelijk. NLT kan een positieve bijdrage leveren aan deze problematiek door de lesstof zo aan te bieden dat deze ook voor meisjes aantrekkelijk is.'

Volgens het zesde kenmerk moet rekening gehouden worden met het verschil tussen havo- en vwo-leerlingen, omdat ze verschillende leerstijlen, belangstelling en kennisniveau hebben. Er wordt een algemene typering gegeven: 'Havo-leerlingen zijn meer productgericht, terwijl vwo-leerlingen sneller gegrepen zijn door de inhoud van de lesstof.'. De argumentatie hiervoor is als volgt: 'Havo-leerlingen hebben meer belangstelling voor praktische en meer toepassingsgerichte onderwerpen die direct aansluiten bij hun belevingswereld; vwo-leerlingen richten zich vaak eerder op theoretische en cultuur-historische onderwerpen.'.

Het document concludeert vervolgens dat het genoemde verschil tussen havo- en vwo-leerlingen op drie aspecten tot een verschillende onderwijsaanpak leidt.

Ten eerste is er in verschil in het soort contexten dat gebruikt zou moeten worden: 'De contexten bij de havo moeten dus vooral gevonden worden in het dagelijks leven, bij het vwo zijn ook wetenschappelijke contexten van belang.'.

Ten tweede is er een verschil in het type opdrachten dat aangeboden zou moeten worden: 'Wat de opdrachten betreft willen havo-leerlingen actiever met de lesstof omgaan, ze willen sneller zelf aan de slag. Bij de havo-modules moet er vooral gebruik gemaakt worden van activerende werkvormen. Bij vwo is klassikale instructie vaker mogelijk. Het vwo vraagt om open opdrachten, terwijl die bij havo meer sturend zijn.'.

Ten derde wordt er is er een verschil in de vaardigheden aangewezen. Dit verschil wordt beargumenteerd aan de hand van het verwachte vervolgonderwijs: 'De meeste havo-leerlingen stromen door naar een hbo-opleiding, terwijl de meeste leerlingen van het vwo naar de universiteit gaan. Bij de lesmodules voor het havo zal daarom het accent vooral op de beroepspraktijk liggen en meer op het ontwerpen, ontwikkelen en toepassen dan op onderzoeken. Bij het vwo gaat het ook om onderzoeken.'.

Het laatste kenmerk stelt een eis aan de onderwerpen van een NLT-module: 'De onderwerpen

van de modules zullen deels interdisciplinair zijn en voor een kleiner deel monodisciplinair voortbouwen op de klassieke bètavakken.'. Onderwijs over security zal vooral bij de eerste categorie passen. Iedereen heeft namelijk, direct of indirect, met security te maken, omdat er in de huidige wereld steeds meer van ICT gebruik gemaakt wordt die ook beveiligd moet zijn.

5.4.2 Toetsing

Het Visiedocument geeft aanbevelingen voor de toetsvormen die gebruikt kunnen worden in NLT-modules. De toetsvormen worden zoveel mogelijk gebruikt in modules die ontwikkeld worden in samenwerking met het Landelijk Ontwikkelpunt NLT. De toetsvormen die genoemd worden zijn:

- 'digitale diagnostische toetsen (zo mogelijk af te nemen via een elektronische leeromgeving)'
- 'een beschrijving van producten (o.a. verslagen en andere presentatievormen van onderzoek) die tijdens de module door de kandidaten opgeleverd dienen te worden, met rubics ter beoordeling van de producten. Hierbij kan ook de mogelijkheid van peer-review (leerlingen beoordelen zichzelf en elkaar) worden gebruikt'
- 'een afsluitende schriftelijke toets met antwoordmodel'

Voor de laatste toetsvorm worden verschillende vraagtypen voorgesteld:

- 'korte gesloten / meerkeuze vragen om kennisdoelen te toetsen'
- 'korte eenvoudige berekeningen en toepassingsvragen'
- 'complexere open opdrachten, waarbij de verworven kennis én vaardigheden in een nieuwe context worden aangeboden. Het kan hierbij ook gaan om de analyse van een set meetgegevens, het ontwerpen van een onderzoek of het uitvoeren van een deel van de ontwerpcyclus'
- 'een of meerdere (keuze) essayvragen, die toetsen in hoeverre de kandidaat in staat is de geleerde concepten te gebruiken voor reflectie op een niet eerder bestudeerde situatie'

De genoemde vraagtypen komen sterk overeen met de categorieën van leren van Blooms taxonomie. In het eerste vraagtype wordt de overeenkomst al letterlijk genoemd met het woord *kennisdoelen*. Dit vraagtype toetst dus de categorie *Kennis*. Het tweede vraagtype geeft ook al letterlijk een aanwijzing met het woord *toepassingsvragen*. Bij toepassingsvragen pas je de geleerde kennis toe, dus dit valt duidelijk onder de categorie *Toepassing*. Ook bij *korte eenvoudige berekeningen* wordt kennis toegepast, want als je weet hoe je de berekening moet uitvoeren, kun je die kennis toepassen door daadwerkelijk die berekening te doen voor nieuwe getallen of andere gegevens.

Het derde vraagtype is eigenlijk niet één vraagtype als je naar de categorieën van Blooms taxonomie kijkt, want het vraagtype gaat over meerdere categorieën. Als de verworven kennis en vaardigheden in een nieuwe context worden aangeboden kan dit nog onder *Toepassing* vallen als er bijvoorbeeld gevraagd wordt om een probleem op te lossen in deze nieuwe context. Maar het kan ook gaan om een categorie van hoger niveau, het is niet specifiek genoeg beschreven om met zekerheid één categorie te kunnen aanwijzen. Analyse van een set meetgegevens is een specifieke vorm van *Analyse*. Het ontwerpen van een onderzoek valt ook onder *Analyse*, dit is namelijk het eerste deel van een volledige analyse, omdat er dan wordt nagedacht hoe de analyse gedaan zal worden. Het uitvoeren van een deel van de ontwerpcyclus zou onder *Toepassing* kunnen vallen, als de ontwerpcyclus helemaal is vastgelegd en de leerling alleen nieuwe gegevens gebruikt bij het uitvoeren van de ontwerpcyclus. Het zou echte ook onder *Synthese* kunnen vallen, als de ontwerpcyclus niet helemaal vastligt en er misschien hooguit wat richtlijnen zijn. De leerling moet dan zelf een ontwerp samenstellen.

Het vierde vraagtype geeft met met woord *reflectie* al een aanwijzing dat hier de categorie *Evaluatie* wordt getoetst. De woorden *op een niet eerder bestudeerde situatie* ondersteunen dat het vraagtype over *Evaluatie* gaat.

Dat de vraagtypen overeen komen met één of meer categorieën van Bloom geeft aan dat het valide soorten vraagtypen zijn, waarin ook echt getoetst wordt of een leerling een bepaald aspect

geleerd heeft. De vraagtypen vallen onder categorieën van verschillende niveaus, wat aangeeft dat ze niet eenzijdig zijn. Niet alle categorieën worden met deze vraagtypen getoetst, wat aangeeft dat er nog wel meer vraagtypen mogelijk zijn. Van de categorieën die wel genoemd zijn, zijn er misschien ook nog andere vraagtypen mogelijk. De genoemde vraagtypen vormen dus geen compleet geheel, maar geven wel een goede opstap naar verschillende manieren van toetsen.

5.5 KNAW

5.5.1 Digitale geletterdheid

Het advies van de Koninklijke Nederlandse Akademie van Wetenschappen (2012) heeft als doel de digitale geletterdheid van de burger te stimuleren. Het advies omschrijft digitale geletterdheid als volgt: 'Digitale geletterdheid is het vermogen digitale informatie en communicatie verstandig te gebruiken en de gevolgen daarvan kritisch te beoordelen. In de 21ste eeuw behoort digitale geletterdheid tot de basisvaardigheden van de ontwikkelde mens. Het is een voorwaarde om te kunnen functioneren in de informatiemaatschappij.'.

Het advies legt vervolgens uit dat digitale geletterdheid thuis hoort in het onderwijs: 'Digitale geletterdheid vraagt, net als taalbeheersing en rekenvaardigheid, om een vormingstraject dat iedereen gedurende langere tijd moet doorlopen. Het onderwerp hoort daarom in het onderwijs thuis.'

Maar digitale geletterdheid komt nog te weinig aan bod in het huidige onderwijs: 'De huidige vakken op dit gebied zijn in veel opzichten onder de maat en bereiden de leerlingen niet op de informatiemaatschappij voor.'

Het advies geeft verschillende aanbevelingen om de huidige stand van zaken te verbeteren. Eén van die aanbevelingen is als volgt: 'Voer een nieuw verplicht vak Informatie & communicatie voor de onderbouw van havo en vwo in. Dit dient een breed en compact inleidend vak te zijn, dat de essentiële aspecten van digitale geletterdheid tot onderwerp heeft.' In de volgende sectie zal worden beargumenteerd dat dit vak op vele punten security-gerelateerd is.

Het advies geeft een argumentatie waarom juist het vak Informatie & communicatie ingevoerd moet worden: 'Waar iedereen voortdurend te maken heeft met digitale informatie en communicatie, ontbreekt bij veel leerlingen in het voortgezet onderwijs een basaal inzicht in de aard en de rol ervan. De commissie pleit daarom voor de invoering van een nieuw verplicht vak Informatie & communicatie (I&C) in de onderbouw van havo en vwo, dat een brede oriëntatie biedt in de basiskennis van digitalisering, computers en computernetwerken en het gebruik en de gevolgen ervan, met aandacht voor de rol van het individu in relatie tot maatschappij en economie en voor de ethische, sociale en juridische aspecten.'.

Omdat het vak Informatie & communicatie bijdraagt aan digitale geletterdheid en, zoals uit de volgende sectie blijkt, de onderwerpen van het vak security-gerelateerd zijn, kan onderwijs over security ook bijdragen aan digitale geletterdheid. Bovengenoemde redenen om digitale geletterdheid te stimuleren en om het vak Informatie & communicatie in te voeren zijn dus ook redenen om onderwijs over security mogelijk te maken.

Behalve de aanbeveling om het vak Informatie & communicatie in te voeren worden er nog meer aanbevelingen gegeven. Zo wordt geadviseerd om het huidige vak Informatica in de bovenbouw te verbeteren en om de interactie met de andere middelbare schoolvakken te stimuleren. Aan de eerste aanbeveling zal de module alleen bijdragen als hij wordt ingezet binnen Informatica. De tweede aanbeveling wordt met de module al in enige mate gerealiseerd, de module wordt namelijk gegeven binnen een algemeen bètavak: NLT. De overige twee aanbevelingen zorgen dat voorgenoemde aanbevelingen gerealiseerd kunnen worden. Er wordt geadviseerd om het opleiden van nieuwe docenten te stimuleren en om samen te werken met de minister van OCW bij het opzetten van de nieuwe vakken.

5.5.2 Onderwerpen van het vak Informatie en Communicatie

In het advies van de Koninklijke Nederlandse Akademie van Wetenschappen (2012) worden bij het vak Informatie & communicatie veel onderwerpen genoemd die security-gerelateerd zijn. Het

advies deelt het vak Informatie & communicatie op in drie componenten: *basiskennis*, *gebruik* en *gedrag*. Per component zal beschreven worden wat het component inhoudt en zal besproken worden welke van de daarbij genoemde onderwerpen (in welke mate) gerelateerd zijn aan security.

Het advies beschrijft de component *basiskennis* als volgt: 'De eerste component omvat de basiskennis van digitalisering, computers en computernetwerken en de daarmee gepaard gaande houding van computational thinking.' *Computational thinking* blijkt dus een belangrijk onderdeel van het component *basiskennis*. Het advies legt uit wat hiermee bedoeld wordt: 'Dit houdt in dat de leerling processen interpreteert in termen van het gestructureerd bewerken van informatie en doorziet hoe communicatie de wereld in een netwerk heeft veranderd waarbij voor mens en machine informatie overal en altijd bereikbaar en uitwisselbaar is.'. Daarna beargumenteert het advies waarom computational thinking belangrijk is: 'Computational thinking is een voorwaarde om de gevolgen, de kansen en de risico's van de digitalisering van informatie en communicatie te kunnen begrijpen en er verantwoord mee te kunnen omgaan.'. Precies om deze rede is een bepaalde mate van computational thinking nodig om security te kunnen toepassen. Om te kunnen bedenken hoe de digitale wereld beveiligd zou moeten worden, is het nodig om te weten hoe deze wereld in elkaar zit.

Van het component *basiskennis* worden vier *essentiële basisconcepten* genoemd:

- informatie, binaire representatie, digitalisering;
- algoritmiek, de principes van programmeren;
- architectuur en werking van computers; databases; wat gebeurt er als je een berekening uitvoert?
- structuur en werking van computernetwerken zoals internet; belang van standaarden zoals IP en HTML; wat gebeurt er als je een e-mail verstuurt?

Het eerste basisconcept is erg algemeen, zeker *informatie*, dat kan binnen bijna elke context wel gebruikt worden. Doel van security is om digitale informatie en diensten te beschermen, volgens (Jacobs, 2011c). Ook wordt security vaak gebruikt om bepaalde informatie over te sturen voor communicatie, bijvoorbeeld met protocollen (Anderson, 2008; Jacobs, 2011c). Informatie past dus prima bij security. *Binaire representatie* wordt in de security gebruikt om data of een sleutel weer te geven. Bij XOR-versleuteling bijvoorbeeld, wordt de XOR-operatie toegepast op de data en de sleutel, die binair worden weergegeven (Enigma, 2013). *Binaire representatie* wordt dus soms gebruikt, maar security heeft niet als doel om uit te leggen wat binaire representatie is. Alleen als het bij een specifieke situatie nodig is zal dit onderwerp dus aan bod komen bij security. *Digitalisering* past dan weer goed bij security, omdat, zoals eerder gezegd, de security als doel heeft digitale informatie en diensten te beschermen.

Bij het tweede basisconcept past vooral het eerste onderdeel binnen security. Er worden vele algoritmes gebruikt binnen de security, neem bijvoorbeeld RSA (Jacobs, 2011c; Enigma, 2013). Maar ook protocollen (Anderson, 2008; Jacobs, 2011c) zou je als algoritmes kunnen zien, aangezien protocollen stap voor stap beschrijven wat er gedaan wordt en algoritmes ook een opeenvolging van stappen zijn, net zoals recepten. Binnen de security wordt wel geprogrammeerd om iets te beveiligen, of in code gezocht naar gaten in de beveiliging van het programma, zie *Interview met docent*, (Anderson, 2008; Jacobs, 2011c). Maar de principes zullen niet snel aan bod komen, security gaat niet over programmeren, maar maakt er alleen gebruik van.

Het derde basisconcept past alleen binnen de security als de security daarvan niet in orde is, of als er juist security toegevoegd moet worden. De architectuur en werking van een computer moet geschikt zijn om security-maatregelen op te kunnen toepassen als de computer ook beveiligd moet worden (Anderson, 2008). Ditzelfde geldt voor databases. Bij het beveiligen van de uitvoering van een berekening kan het misschien van belang zijn om te zorgen dat de tussenuitkomsten en de einduitkomst niet veranderd kan worden.

Het vierde basisconcept past weer iets beter bij security dan het derde basisconcept, omdat bij de onderdelen van dit concept vaker security toegepast wordt. Bij het opzetten van het Internet is niet zo goed nagedacht over de security, waardoor hier achteraf iets aan gedaan moest worden

(Jacobs, 2011c). Toen internetprotocollen als IP en HTML bedacht werden, was het hebben van security nog niet zo'n prominente eis. Als je *wat gebeurt er als je een e-mail verstuurt?* bijvoorbeeld opvat als *wie kan mijn e-mail lezen?*, dan gaat het over security. PGP (Jacobs, 2011c; Enigma, 2013) is bijvoorbeeld een manier om e-mail versleuteld te versturen, zodat niemand kan meelezen.

De tweede component *gebruik* wordt als volgt beschreven: 'De tweede component betreft het gebruik van digitale informatie en communicatie en van het gereedschap dat daartoe beschikbaar is. Digitaal geletterde leerlingen kunnen omgaan met standaardsoftware en -apparatuur en tonen daarbij een kritische houding. Ze zijn vertrouwd met de denkwijze van de ICT als oplossingsgerichte discipline. Zij beseffen dat ICT grote en vaak verstorende gevolgen heeft voor bijna alle aspecten van het menselijk handelen. In het onderwijs zijn hiervan talloze voorbeelden te vinden, die vaak een relatie leggen met andere vakken.' Deze beschrijving van de component *gebruik* bevat vele elementen die belangrijk zijn in de security. Een kritische houding is bijvoorbeeld erg belangrijk, zoals bijvoorbeeld blijkt uit (Jacobs, 2011c) en *Interview met docent*. Security is bij uitstek een oplossingsgerichte discipline, men gaat zelfs opzoek naar mogelijke aanvallen/gaten, waarna uitgezocht wordt hoe die aanval voorkomen kan worden, zoals blijkt uit *Interview met docent* en (Jacobs, 2011b). Een voorbeeld van een verstorend gevolg is de schending van privacy. Security probeert dit tegen te gaan (Anderson, 2008; Jacobs, 2011c).

Van het component *gebruik* worden vijf *karakteristieke onderwerpen* genoemd:

- ontwikkeling in perspectief: geschiedenis van gedachtegoed, techniek en toepassingen; onvoorspelbaarheid van de digitale revolutie;
- verzamelen van informatie: bronnen, zoekmachines; presentatie van informatie; betrouwbaarheid en kwaliteit van informatiebronnen;
- opslaan en beveiligen van informatie; waar staan de gegevens eigenlijk? wie kan erbij?
- systemen: kwetsbaarheid (virussen, hacking, spam); internetdiensten, encryptie; applicaties voor mobiele apparatuur;
- sociale netwerken; hoe wordt je profiel opgebouwd? hoe worden advertenties op jouw voorkeuren afgestemd?

Al in de tijd van de Grieken werden er methoden gebruikt om berichten te versleutelen, maar vaak bleken deze methoden niet veilig genoeg. Er werden in de loop van de tijd steeds nieuwe methoden ontwikkeld. Toen de computer kwam, moest er ook nog rekening gehouden worden met de rekenkracht van de computer, omdat daarmee vercijferde berichten die met de hand niet te kraken waren, met de computer nu wel gekraakt konden worden (Enigma, 2013; Jacobs, 2011c). Over het eerste onderdeel van dit component is in de security dus wel wat te zeggen.

Het tweede onderwerp heeft niet veel te maken met security, behalve als er wat verder gekeken wordt. Dan kan bijvoorbeeld de beschikbaarheid van de informatie een probleem zijn, of de privacy geschonden wordt door het bekend maken of bij elkaar zetten van informatie. Maar uit wat er voor deelonderwerpen genoemd worden blijkt dat dit niet de hoofdzaak is, dus misschien wordt dit helemaal niet bedoeld.

De derde onderwerp sluit weer goed aan bij security, dat blijkt al uit de woorden *beveiligen van informatie*. Zoals eerder gezegd heeft de security als doel om digitale informatie (en diensten) te beschermen (Jacobs, 2011c). Dus ook als die informatie is opgeslagen. Wie er bij kan wordt bepaald door de toegangscontrole die wordt gebruikt om iemand toe te laten tot die informatie. Toegangscontrole is een groot onderwerp binnen de security (Anderson, 2008; Jacobs, 2011c).

Het vierde onderwerp sluit ook goed aan bij security. Security zorgt voor bescherming, dus dit betekent dat de kwetsbaarheid van systemen zo minimaal mogelijk wordt gemaakt, dus dat virussen, hacking en spam zoveel mogelijk worden tegengegaan of voorkomen (Anderson, 2008). Internetdiensten vallen onder *digitale diensten* (Jacobs, 2011c) en applicaties op mobiele appartuur vallen ook onder deze *digitale diensten* (Jacobs, 2011c). Encryptie is onderdeel van cryptografie, een groot onderwerp binnen de security (Enigma, 2013; Anderson, 2008; Jacobs, 2011c).

Het vijfde onderwerp is samen te vatten als *privacy*. De informatie op sociale netwerken is vaak voor veel mensen zichtbaar, waardoor er privacy wordt weggegeven (Anderson, 2008). Bedrijven vinden dit soort informatie interessant omdat ze er geld mee kunnen verdienen, dus bouwen ze profielen op waardoor ze in staat zijn gerichte advertenties te gebruiken (Anderson, 2008).

Het derde component *gedrag* wordt door het advies als volgt beschreven: 'De derde component betreft het gedrag en de rol van het individu. De manier waarop de digitalisering van informatie en communicatie ons leven en onze relatie met anderen beïnvloedt, heeft ethische, sociale, juridische en economische aspecten. Het hanteren van normen en waarden, het inschatten van kansen en risico's en het afwegen van eigendom, privacy en vrijheid zijn voortdurende uitdagingen om actief en verantwoord deel te nemen aan de informatiemaatschappij.' Security past ook bij deze component. Security bepaald mede hoe de digitalisering van informatie en communicatie tot uiting komt in de maatschappij, security is een erg interdisciplinair vakgebied (Jacobs, 2011c; Anderson, 2008). Onderwerpen als privacy en vrijheid vallen duidelijk binnen de security (Anderson, 2008).

Bij het component *gedrag* worden vier *wezenlijke aspecten* aangegeven:

- ethische aspecten: normen en waarden; hoe ga je met je identiteit en met die van anderen om?
- sociale aspecten: interactie in sociale netwerken, privacy, cyberpesten, cybercriminaliteit;
- juridische aspecten: eigendom, copyright, auteursrecht, downloaden;
- economische aspecten: economie van de informatie, persoonsgegevens als ruilmiddel.

De onderwerpen die bij *ethische aspecten* genoemd worden, vallen niet heel duidelijk binnen het vakgebied, maar er zijn wel degelijk ethische aspecten waar men in de security mee te maken heeft. Als er bijvoorbeeld een beveiligingslek wordt gevonden in een systeem, waardoor er ongeoorloofd toegang wordt verkregen tot bijvoorbeeld persoonsgegevens, dient dit lek op een goede manier bekend gemaakt te worden. Security heeft tenslotte als doel om digitale informatie en hiermee privacy te beschermen (Jacobs, 2011c).

Van de onderwerpen die bij *sociale aspecten* genoemd worden vallen vooral de algemenere onderwerpen binnen de security. Zoals al eerder gezegd is privacy onderdeel van de security. Cybercriminaliteit is het ondermijnen van de security, de security heeft als doel deze criminaliteit tegen te gaan (Anderson, 2008). Het zorgen voor een aangename interactie in sociale netwerken en het voorkomen van schending van privacy zijn dingen die echt op het sociale vlak zitten, dit kan makkelijker opgelost worden met bijvoorbeeld moderators dan een technische oplossing.

Door security te gebruiken is het mogelijk om digitale informatie te beveiligen, waardoor eigendom, copyright en auteursrecht beschermd kan worden en downloaden voorkomen kan worden (Anderson, 2008). Security zal er vooral voor zorgen dat de wet gehandhaafd kan worden. De vraag wat er (juridisch) wel en niet mag valt buiten de security.

De onderwerpen die genoemd worden bij *economische aspecten* vallen weer duidelijk binnen de security. Security probeert digitale informatie te beschermen, terwijl de economie juist profiteert van deze informatie. Dit leidt tot botsingen (Anderson, 2008).

Veel van de onderwerpen die onderdeel zijn van het vak Informatie & communicatie zijn dus gerelateerd met de security. Vaak direct, maar soms ook indirect door naar het security-aspect van het onderwerp te kijken.

5.6 Vergelijking van resultaten

In voorgaande secties van dit hoofdstuk zijn de resultaten weergegeven per bron. Hierbij komen veel elementen naar voren die in verschillende bronnen aan bod komen. Deze elementen worden hieronder per deelvraag met elkaar vergeleken.

5.6.1 Leerdoelen

In de resultaten zijn veel algemene motivaties te vinden om onderwijs te geven over security. In de resultaten over het *Visiedocument* bijvoorbeeld wordt beargumenteerd dat ICT, en daarmee security, een grote rol speelt in de wetenschap en technologie en tot uiting komt in vele toepassingen die we in het dagelijks leven gebruiken. In de resultaten over *Het vak Security* wordt dit beeld met de studiegids (*Studiegids Security*, 2011) bevestigd: wereldwijd wordt erkend dat security van groot belang is voor alle informatietechnologieën. Bovendien komen in de collegeslides (Jacobs, 2011c) veel (praktijk)toepassingen aan bod.

De resultaten over het advies van de Koninklijke Nederlandse Akademie van Wetenschappen (2012) sluiten hierop aan. Er wordt hierbij een brug geslagen dus de algemene motivatie om te onderwijzen in security en de motivatie om specifieke onderwerpen aan bod te laten komen in het onderwijs. Digitale geletterdheid is een voorwaarde om te kunnen functioneren in de informatiemaatschappij, met al die toepassingen zoals genoemd in *Visiedocument*. Een manier om deze geletterdheid te stimuleren is door het invoeren van het vak Informatie & communicatie, een vak waarin de essentiële aspecten van digitale geletterdheid aan bod komen. Deze essentiële aspecten blijken veelal security-gerelateerd. Hieruit volgt dat onderwijs over security dus kan bijdragen aan digitale geletterdheid, waardoor onderwijs hierover belangrijk is voor de maatschappij. De algemenere gebieden *basiskennis*, *gebruik* en *gedrag* met hun specifieke onderwerpen vormen zo een motivatie om deze onderwerpen aan bod te laten komen in onderwijs over security.

Dat security belangrijk is voor de maatschappij komt ook naar voren als *Het vak Security* gekoppeld wordt aan *KNAW*. Het eerste leerdoel van *Het vak Security* komt overeen met het eerste onderdeel *computational thinking* van Informatie & communicatie, en dan vooral waarvoor men *computational thinking* nodig heeft. Het kunnen begrijpen en omgaan met gevolgen, kansen en risico's van de digitalisering heeft overeenkomsten met het herkennen van situaties waarin security een rol speelt, want die gevolgen, kansen en risico's zijn zichtbaar in de situaties waar security een rol speelt. Het vierde leerdoel van *Het vak Security* bevestigt dit door te vragen om herkenning en analyse van de sociale en organisatorische gevolgen van security-technologieën. Die gevolgen zijn kennelijk volop aanwezig in de wereld.

Het vervolg geeft een overzicht van specifieke leerdoelen en bijbehorende onderwerpen die bij de resultaten naar voren zijn gekomen. Als uitgangspunt worden *Het vak Security* en *KNAW* genomen, omdat de eerste een goed beeld van onderwijs over security geeft en de tweede de maatschappelijk relevante aspecten aangeeft. De resultaten van *Enigma* en *Interview met docent* zijn specifieker en worden gebruikt als ondersteuning.

Het onderwerp security doelen is onderdeel van twee van de vier leerdoelen van *Het vak Security*. Hieruit blijkt dat dit een onderwerp erg belangrijk wordt gevonden. Het onderwerp *security eisen* in *Interview met docent* komt overeen met de security doelen, want confidentialiteit en integriteit zijn precies twee security doelen. Volgens *Interview met docent* is de reden om die eisen te leren dat je door naar de eisen te kijken van een systeem dat je gaat bouwen, je van te voren al nadenkt over de security van het systeem, dus de risico's die je loopt, in plaats van achteraf hier nog maatregelen voor te moeten nemen.

Aan het onderwerp *privacy* dat in het vierde leerdoel van het *Het vak Security* genoemd wordt, wordt ook belang gehecht in *KNAW*. Daarin is *privacy* één van de *wezenlijke aspecten* van het onderdeel *gedrag*. Bovendien hangen vele onderwerpen die daar ook genoemd worden mee samen, bijvoorbeeld *persoonsgegevens als ruilmiddel*, (*interactie in*) *sociale netwerken* en *hoe ga je met je identiteit en met die van anderen om?*. Dit soort onderwerpen worden sterk beïnvloed door de security-maatregelen die zijn genomen. Bovendien is (bescherming van) de eigen privacy iets waar iedereen wel in meer of mindere mate mee te maken heeft, wat het een erg maatschappelijk onderwerp maakt.

Een security-maatregel die veel wordt genomen om privacy, of in het algemeen digitale informatie en diensten te beschermen, is het gebruik van wachtwoorden. De *KNAW* noemt als onderwerp het beveiligen van informatie. Wachtwoorden worden ook genoemd als onderwerp in *Het vak Security*. Wachtwoorden worden erg veel gebruikt, waardoor het belangrijk is dat er ook goede wachtwoorden worden gebruikt. Want als een wachtwoord te raden is gaat de authenticatie

fout en heeft iemand onterecht toegang gekregen. Wachtwoorden vallen dus binnen het onderwerp authenticatie, een onderwerp uit *Het vak Security* en *Enigma*, maar authenticatie wordt niet in *KNAW* genoemd, omdat het een vakterm is.

In *Het vak Security* en *Enigma* wordt vooral gekeken vanuit de beveiligingsmaatregelen die je kunt nemen, zoals netwerkbeveiliging, PGP en versleuteling, en specifieke aanvallen daarop. In *KNAW* wordt juist gekeken naar veel algemenere de antimaatregelen die (cyber)criminelen kunnen nemen om security te omzeilen, namelijk de kwetsbaarheid door virussen, hacking en spam. Ook juridische maatregelen worden genoemd, bijvoorbeeld copyright en auteursrecht.

Daarnaast zijn er ook maatregelen die beveiliging juist mogelijk maken. Dit was een onderwerp dat veel naar voren kwam in *Resultaten*, vooral bij de meer inhoudelijke bronnen. Zowel in *Het vak Security* en *Enigma* was er één onderwerp dat veel aan bod kwam. Bij *Het vak Security* was dit protocollen en bij *Enigma* was dit asymmetrische versleuteling. Om een toepassing van asymmetrische versleuteling, RSA, te kunnen gebruiken, is best veel (voor)kennis nodig over modulorekenen en het gebruik daarvan blijkt uit (Jacobs, 2011c; Enigma, 2013). Dit terwijl modulorekenen alleen maar een middel is om security te kunnen toepassen en geen doel op zichzelf. Modulorekenen valt onder algebra. Deze voorkennis wordt genoemd in de studiegids van *Het vak Security*, aangezien bij dit vak al van basiskennis over modulorekenen uit wordt gegaan. Een manier om deze voorkennis niet nodig te hebben of het geven van onderwijs over modulorekenen te ontwijken ontstaat door de twee onderwerpen die veel aan bod komen in *Het vak Security* en *Enigma* te combineren. Protocollen maken namelijk vaak gebruik van cryptografie zonder dat men hoeft te weten hoe deze cryptografie precies werkt. Asymmetrische versleuteling kan dus ook prima aan bod komen in het onderwijs door alleen de concepten uit te leggen, waarna gelijk wordt doorgegaan naar protocollen die gebruik maken van asymmetrische versleuteling.

Bij protocollen is het belangrijk dat ze ook veilig zijn, anders heb je er niet veel aan. Deze veiligheid is een onderwerp bij *Het vak Security*, maar ook bij *Interview met docent*, alleen wordt er dan naar de onveiligheid gekeken, dus naar wat er typisch mis gaat. Ervaring met de dingen die misgaan blijkt erg belangrijk. Bij de twee vakken die de docent in *Interview met docent* geeft is dit een belangrijk thema. Deze ervaring kan in de context van protocollen bijvoorbeeld opgedaan worden door aanvallen erop te bedenken of juist te beargumenteren waarom het protocol veilig is. Ook in *Enigma* worden bepaalde soorten aanvallen uitgelegd: de brute force attack en de man-in-the-middle attack. Het bedenken van aanvallen en het beoordelen van de veiligheid is dus een belangrijk aspect van protocollen.

Een overeenkomst tussen *KNAW* en *Interview met docent* is dat bij beide resultaten een kritische houding als belangrijk wordt verondersteld. In *Interview met docent* wordt uitgelegd wat dat dat in de security vooral tot uiting komt doordat er naar gaten ofwel aanvallen gezocht wordt op systemen. Als de leerling gevraagd wordt om aanvallen te bedenken op protocollen wordt deze kritische houding dus aangesproken. Hiermee wordt gestimuleerd dat de leerling creatief nadenkt over het probleem.

Een andere overeenkomst tussen *Het vak Security* en *Enigma* is dat symmetrische versleuteling aan bod komt vóór asymmetrische versleuteling. Dit geeft een indicatie dat de eerste voorkennis vormt voor de tweede. Als asymmetrische versleuteling aan bod komt in het onderwijs, moet symmetrische versleuteling daardoor ook aan bod komen, en wel ervoor. Zoals al in *Het vak Security* gezegd is, is het concept van symmetrische versleuteling redelijk laagdrempelig, omdat iedereen wel eens geheimschrift gebruikt heeft. Symmetrische versleuteling kan hierdoor een opstap vormen naar asymmetrische versleuteling. Ook werd symmetrische versleuteling eerder dan asymmetrische versleuteling uitgevonden, waardoor met deze volgorde ook mooi de ontwikkeling van cryptografie weergegeven kan worden, zoals in *Enigma* gedaan is. Het geschiedenisaspect dat in *KNAW* genoemd wordt (ontwikkeling in perspectief, geschiedenis van gedachtegoed etc.) komt zo ook aan bod.

In het algemeen blijkt cryptografie wel een belangrijk onderwerp te zijn. *Enigma* heeft een hele module aan dit onderwerp besteed. Ook bij *Het vak Security* gaat een groot deel van het vak over cryptografie. Bovendien is *encryptie* een van de onderwerpen die in *KNAW* genoemd wordt. Ook in *Interview met docent* wordt cryptografie genoemd als beveiligingstechniek.

Er zijn nog een aantal onderwerpen die hierboven niet aan bod zijn gekomen. Deze onderwerpen

waren dan minder interessant, omdat ze niet in meer dan één van de resultaten naar voren kwamen. Een mogelijke verklaring hiervoor is dat die onderwerpen dan heel specifiek waren, waardoor ze niet kenmerkend waren of dat ze binnen andere onderwerpen vielen.

5.6.2 Begrip van leerlingen

Alleen bij het resultaat *Interview met docent* werd ingegaan op het begrip dat de studenten hadden van het aangeboden onderwijs. Dit is wel logisch, want alle andere bronnen beschrijven schriftelijk hoe het onderwijs in elkaar zit. Er wordt achteraf geen oordeel gegeven over hoe het onderwijs verliep. Er kan dus geen vergelijking gemaakt worden met andere bronnen. Het interview geeft maar één voorbeeld van een probleem, namelijk dat leerlingen er wel aan denken om confidentialiteit te waarborgen, maar vaak vergeten om ook integriteit te waarborgen.

5.6.3 Onderwijsaanpak

In *Visiedocument* worden een aantal algemene onderwijsaanpakken aanbevolen. Vanuit deze onderwijsaanpakken zal ingegaan worden op de aanpakken die aan het licht zijn gekomen bij de andere resultaten.

Ten eerste wordt in *Visiedocument* erop gewezen dat structuur van belang is. Bij *Enigma* komt er een duidelijke structuur naar voren door de indeling van de module in hoofdstukken en paragrafen. Bovendien wordt in het eerste hoofdstuk uitgelegd wat de gedachte is achter die structuur. Bij *Het vak Security* is de structuur wat minder zichtbaar, al komen de onderwerpen wel één voor één aan bod, waardoor de grenzen vaak makkelijk te zien zijn. Belangrijk is dus in ieder geval dat het onderscheid tussen de verschillende onderwerpen duidelijk is. Tussenkopjes zoals bij *Enigma* gebruikt worden, kunnen hieraan bijdragen.

Ten tweede wordt in *Visiedocument* een activerende didactiek geadviseerd die de leerling de regie geeft over het eigen leerproces. Deze aanpak komt sterk overeen met het constructivisme. In *Interview met docent* wordt belang gehecht aan deze activerende didactiek: het is belangrijk dat de leerlingen zelf aan de slag gaan. In *Het vak Security* en *Enigma* komt dit niet heel duidelijk naar voren. Wel stellen beide lesmethodes een grote set aan opdrachten beschikbaar waardoor de leerling zelf met het geleerde aan de slag gaat. Verder worden bij *Het vak Security* veel toepassingen uit de praktijk besproken, waardoor de leerling aangemoedigd wordt zelf verbanden te leggen tussen de geleerde concepten en de praktijk. Dit komt precies overeen met het leren van concepten binnen contexten, de derde aanbeveling in *Visiedocument*. Alleen wordt bij *Het vak Security* vaak eerst wat theorie besproken en daarna pas ingegaan op voorbeelden en toepassingen. In *Enigma* wordt door de hele module heen de context *ontwikkeling van de cryptografie* gebruikt. Er wordt begonnen met technieken uit de oudheid, waarna men uiteindelijk uitkomt bij de huidige tijd. *Interview met docent* sluit ook aan op concepten leren binnen contexten: er wordt altijd begonnen met een voorbeeld om de intuïtie duidelijk te maken. Daarna wordt er op de details ingegaan, waarna meestal nog even wordt teruggekoppeld naar de intuïtie.

Verder wordt in *Visiedocument* aandacht besteed aan de doelgroep. Het onderwijs moet niet alleen voor jongens, maar ook voor meisjes aantrekkelijk zijn. Dit kan bijvoorbeeld door geen typische jongens-voorbeelden te geven. Ook helpt het als er maatschappelijke onderwerpen of toepassingen aan bod komen, daar kan iedereen zich wel iets bij voorstellen. In *Het vak Security* komen al veel van dit soort voorbeelden en toepassingen aan bod. Ook hebben de onderwerpen die in *KNAW* aanbevolen worden veelal een maatschappelijk aspect.

Het is belangrijk om onderscheid te maken tussen havo- en vwo-leerlingen in de aanpak van het onderwijs. De inhoudelijke bronnen die voor de resultaten gebruikt zijn, zijn allemaal bedoeld voor het vwo of wetenschappelijk onderwijs. Het is wel mogelijk om de moeilijke aspecten van het onderwijs minder aan bod te laten komen, maar bij onderwerpen als protocollen zijn de opdrachten al snel uitdagend. Hierdoor is de inhoud die hiervoor is besproken meer geschikt voor vwo-leerlingen.

5.6.4 Toetsing

In *Visiedocument* worden drie toetsvormen genoemd: een digitale diagnostische toets, beschrijving van producten en een afsluitende schriftelijke toets (met antwoordmodel). Bij *Interview met docent* wordt genoemd dat studenten hun product documenteren op een wiki, dus dat komt overeen met de tweede toetsvorm. Ook moeten de studenten practica doen met tools. Practicum wordt niet genoemd als toetsvorm in *Visiedocument*. Ook de opdrachten van *Enigma* en *Het vak Security* worden niet genoemd als toetsvorm. Misschien is in *Visiedocument* toetsing nauwer opgevat, waarbij het tussendoor (zonder cijfer) toetsen van leerlingen niet is meegenomen.

De afsluitende schriftelijke toets wordt gebruikt bij *Enigma*, *Het vak Security* en *Interview met docent*. Bij *Interview met docent* gaat het tentamen van het vak *Software Security* over de theoretische aspecten van het vak. Te verwachten is dat dit tentamen dan veel kennisvragen bevat, zoals het eerste vraagtype dat in *Visiedocument* genoemd wordt, alleen hoeven dat dan geen gesloten of meerkeuze vragen te zijn. De korte toepassingsvragen van het tweede vraagtype zijn dan ook mogelijk door bijvoorbeeld te vragen om bepaalde theoretische aspecten toe te passen in een nieuwe situatie. Hiermee zal de categorie *Toepassing* van Blooms taxonomie de categorie van het hoogste niveau zijn dat gehaald wordt. Maar bij de (praktische) opdrachten worden categorieën van hogere niveaus gehaald. Bij het bouwen van een hardware-oplossing bijvoorbeeld, wordt *Synthese* gehaald, want de studenten moeten dan met behulp van de dingen die ze geleerd hebben een oplossing bouwen. *Evaluatie* komt duidelijk aan bod met de Code-review.

Zoals blijkt uit de resultaten in *Enigma* worden in de *Toets* vooral kennisdoelen getoetst. Dit komt dus vooral overeen met het eerste vraagtype van *Visiedocument*, alleen zijn de vragen open in plaats van gesloten of meerkeuze. De *Inzicht*-vragen zijn ook erg kort en vragen om uitleg, dus passen daardoor ook beter bij het eerste vraagtype. De vragen die in de categorie *Toepassing* vallen zijn korte toepassingsvragen en komen dus overeen met het tweede vraagtype van *Visiedocument*. De vraag die de categorie *Synthese* heeft, is ook kort, maar wel wat moeilijker, dus dat is wel op te vatten als een complexere open opdracht waarbij een ontwerp wordt gemaakt. Zoals al gezegd toetsen de opdrachten van *Enigma* wel vaker een categorie van hoger niveau (vooral *Toepassing*).

De vragen van het tentamen van *Het vak Security* toetsen op *Toepassing* of een categorie van hoger niveau. De korte toepassingsvragen vallen onder het tweede vraagtype, maar veel vragen zijn ook uitgebreider en bieden een nieuwe context en/of nieuwe informatie waardoor ze overeen komen met het derde vraagtype in *Visiedocument*. Zoals aangegeven in *Visiedocument* valt het vierde vraagtype, reflectie geven op een niet eerder bestudeerde situatie met behulp van de geleerde concepten, onder *Evaluatie*. De vragen uit het tentamen van *Het vak Security* die bij de categorie *Evaluatie* passen komen hierdoor overeen met het vierde vraagtype.

De eerste twee simpelere vraagtypen van *Visiedocument* worden dus voornamelijk gebruikt bij de afsluitende schriftelijke toets van *Enigma* en *Interview met docent*, terwijl bij *Het vak Security* ook de andere twee vraagtypen aan bod komen. Een verklaring hiervoor is dat *Enigma* voor middelbare scholieren is bedoeld en *Het vak Security* voor (universitaire) studenten, waarvan je ook mag verwachten dat ze moeilijkere vragen aankunnen. Bovendien kwamen de toetsvragen goed overeen met de opgestelde leerdoelen. Het tentamen dat genoemd werd in *Interview met docent* was bedoeld om de theorie te toetsen, de categorieën van hogere niveaus werden met opdrachten getest.

6 Conclusie en discussie

Zoals uitgelegd in *Probleemstelling* is de onderzoeksvraag concreter gemaakt met vier deelvragen. Deze vier deelvragen zullen in dit hoofdstuk beantwoord worden. Samen vormen ze het antwoord op de onderzoeksvraag. Waar dat van toepassing is zullen punten van discussie aangekaart worden. Tenslotte wordt besproken hoe deze antwoorden gebruikt zullen worden voor de ontwikkeling van de module.

6.1 Leerdoelen

Er zijn een aantal algemene motivaties om onderwijs te geven over security. Ten eerste speelt security een grote rol in wetenschap en technologie, waardoor het tot uiting komt in vele toepassingen in het dagelijks leven. Ten tweede draagt security bij aan de digitale geletterdheid van leerlingen, een vaardigheid die nodig is om goed te kunnen functioneren in de huidige informatiemaatschappij. Ten derde helpt security om de gevolgen, kansen en risico's van digitalisering te kunnen inschatten.

In het onderzoek zijn een aantal specifieke leerdoelen en onderwerpen naar voren gekomen, die kenmerkend zijn voor onderwijs over security. De security doelen vormen een manier om naar de werkelijkheid te kijken en deze doelen ook te gebruiken bij het construeren van toepassingen. Security-maatregelen hebben vaak grote invloed op privacy waardoor het belangrijk is dit aan bod te laten komen binnen onderwijs over security. Authenticatie is een manier om gevoelige informatie en daarmee ook privacy te beschermen. Daarentegen zijn er ook maatregelen die een bedreiging kunnen vormen voor security, zoals malware. Om hiertegen bescherming te kunnen bieden is het nodig om hier iets vanaf te weten. Daarnaast zijn de technieken die zorgen voor een bepaalde beveiliging erg belangrijk. Door deze technieken wordt security namelijk mogelijk gemaakt. Cryptografie zorgt voor de bouwstenen van die technieken. Protocollen gebruiken de bouwstenen van de cryptografie om zo'n beveiligingstechniek mogelijk te maken. Cryptografie bestaat uit twee hoofdonderdelen: symmetrische en asymmetrische cryptografie. Deze twee onderdelen verschillen van elkaar, maar komen ook op punten overeen, doordat ze beiden over cryptografie gaan. Ten slotte is het belangrijk om met een kritsiche houding naar maatregelen en toepassingen te kijken die security waarborgen, omdat één klein foutje gevolgen kan hebben voor de beveiliging van het hele systeem.

6.2 Begrip van leerlingen

Dit onderzoek heeft maar één probleem van leerlingen bij het leren van security opgeleverd. Leerlingen blijken vooral te denken aan het versleutelen van informatie, dus het waarborgen van confidentialiteit. Hierdoor vergeten ze andere security doelen zoals integriteit, terwijl deze soms zelfs belangrijker zijn dan confidentialiteit. Dit probleem is maar in één bron naar voren gekomen, waardoor het antwoord op deze deelvraag op één bron is gebaseerd. Dit zal daarom nooit een compleet beeld geven, waardoor verder onderzoek hierover nodig is.

6.3 Onderwijsaanpak

Het is belangrijk om een goede structuur aan te brengen in het onderwijs, want dit biedt houvast voor de leerlingen. Verder helpen een activerende didactiek en het leren van concepten binnen contexten een leerling bij het leren. Ook is het belangrijk om rekening te houden met de doelgroep. Het onderwijs dient geschikt te zijn voor zowel jongens als meisjes. Daarnaast moet er rekening gehouden worden met het niveau van de leerlingen. Voor havo-leerlingen is een praktijkgerichte aanpak geschikt, voor vwo-leerlingen een aanpak waarbij ook onderzoek een rol speelt. De leerdoelen en onderwerpen die hiervoor besproken zijn, passen beter bij vwo-leerlingen.

6.4 Toetsing

Het maken van opdrachten blijkt een goede manier te zijn om de leerlingen te toetsen. Uitgebreidere vormen als practica en grotere opdrachten met verslagen zijn ook een mogelijkheid, als dit aansluit op de inhoud van het onderwijs. Een schriftelijke afsluitende toets blijkt een veelgebruikte manier om te bepalen wat een leerling geleerd heeft door het onderwijs. Hierbij moet er goed gelet worden op het niveau van de toetsvragen. Behalve toetsvragen van een lager niveau dienen er ook toetsvragen van een hoger niveau gebruikt te worden. Hierdoor komen ook de moeilijkere dingen uit het onderwijs aan bod in de toetsvragen.

6.5 Ontwikkeling van module

Bovenstaande antwoorden op de deelvragen zijn te vertalen naar uitgangspunten voor de module. Vanwege de resultaten en conclusies over leerdoelen en onderwerpen, zal de module onderwijs bevatten over de volgende onderdelen:

1. Inleiding op security met security doelen
2. Symmetrische cryptografie met versleuteltechnieken uit verschillende tijden
3. Asymmetrische cryptografie, gebruikt voor protocollen.
4. Authenticatie, inclusief wachtwoorden
5. Malware en andere kwetsbaarheden door (gebruik van) computers
6. Privacy, inclusief sociale netwerken en persoonsgegeven als manier om geld te verdienen

Hiermee wordt bijgedragen aan onderwijs van digitale geletterdheid en maatschappelijke aspecten, maar wordt ook ingegaan op de vakinhoudelijke aspecten van security.

Het probleem dat leerlingen integriteit vergeten, kan worden voorkomen door de security doelen als eerste te presenteren, voordat iets gezegd wordt over versleutelen. De security doelen kunnen hierbij met evenveel aandacht voor elk doel gepresenteerd worden, zodat de leerling niet aangemoedigd wordt om het vooroordeel op te lopen dat het vooral om confidentialiteit gaat.

De leerdoelen en onderwerpen die zijn gevonden bij dit onderzoek passen beter bij het vwo. Omdat de leerdoelen en onderwerpen van de module zijn afgeleid zijn uit de resultaten van dit onderzoek, zal de module ook bedoeld zijn voor vwo-leerlingen. De maatschappelijke onderwerpen van de module helpen om het ook relevant te maken voor meisjes, maar geven wel genoeg uitdaging. Er zullen zoveel mogelijk voorbeelden en contexten gegeven worden waarmee de inhoud duidelijk wordt gemaakt. De leerling zal actief bij het onderwijs betrokken worden door een open, aansprekende schrijfstijl te gebruiken en de leerlingen zelf aan de slag te laten gaan met opdrachten. Kopjes zullen helpen structuur te bieden.

Voor de module zal een toets samengesteld worden met vragen die vergelijkbaar zijn met de opdrachten. Zowel bij de opdrachten als de toetsvragen zal er voor gezorgd worden dat ook de Bloom-categorieën van hogere niveaus aan bod komen.

In de *Appendix* is een eerste versie van de module te vinden.

Literatuur

Anderson, R. (2008). *Security engineering.* John Wiley & Sons.

Bloom, B. S. (1956). *Taxonomy of educational objectives: The classification of educational goals.*

Bransford, J. D., Brown, A. L., Cocking, R. R. et al. (2000). *How people learn.* National Academy Press Washington, DC.

Enigma. (2013). *www.enigma-online.nl.*

Jacobs, B. (2011a, 20 January). *Exam security.* (www.thalia.nu/onderwijs/tentamenbundel/?action=download&id=149)

Jacobs, B. (2011b). *Security assignments.* (Klik op de link 'exercises' op http://www.ru.nl/ds/education/courses/security-2011/)

Jacobs, B. (2011c). *Security collegeslides.* (http://www.ru.nl/ds/education/courses/security-2011/)

Koninklijke Nederlandse Akademie van Wetenschappen. (2012, December). *Digitale geletterdheid in het voortgezet onderwijs, vaardigheden en attitudes voor de 21ste eeuw.*

Landelijk Coördinatiepunt NLT. (2013). *http://betavak-nlt.nl/landelijk/overnlt/.*

Loughran, J., Mulhall, P. & Berry, A. (2004). In search of pedagogical content knowledge in science: Developing ways of articulating and documenting professional practice. *Journal of Research in Science Teaching*, *41*(4), 370–391.

Magnusson, S., Krajcik, J. & Borko, H. (1999). Nature, sources, and development of pedagogical content knowledge for science teaching. *Examining pedagogical content knowledge: The construct and its implications for science education*, *6*, 95–132.

Minister van Onderwijs, Cultuur en Wetenschap. (2011, mei). *Staatscourant nr. 9161.*

Procedure ontwikkelen en certificeren externe nlt-modules. (2012). (betavak-nlt.nl/les/Ontwikkeling-modules)

Rouwenhorst, M., Praagman, F., Stevens, Y., Wagner, C. & Griffioen, A. (2010). *NLT-worden de doelen waargemaakt?* [Praktijkgericht Onderzoek].

Saeli, M. (2012). Teaching programming for secondary school: a pedagogical content knowledge based approach. *Technische Universiteit Eindhoven*.

Shulman, L. S. (1986). Those who understand: Knowledge growth in teaching. *Educational researcher*, *15*(2), 4–14.

Studiegids security. (2011). (http://www.studiegids.science.ru.nl/2011/science/prospectus/inf_ba/contents/course/28205/)

Stuurgroep Natuur, Leven en Technologie. (2007, april). *Contouren van een nieuw bètavak: Visie op een interdisciplinair vak: Natuur, leven en technologie.*

7 Appendix

7.1 Het uitgeschreven interview

Hieronder staat het uitgeschreven interview met Erik Poll. Alleen de haperingen, stiltes en bevestigende woorden als *Ja* zijn weggelaten.

Ik wil je graag interviewen over het leren van security over studenten. Kun je misschien een punt noemen wat je belangrijk vind, wat is een belangrijk onderwerp, gewoon eentje uitkiezen?
Een onderwerp...? Welke vakken geef je bijvoorbeeld?
Ik geef Hardware security en software security. Daar kan ik een beetje alles in doen.
Wat komt er zoal aan bod?
Standaard manieren om security eisen te inventariseren en standaard manieren om security eisen te garanderen, technieken ter beveiliging die je kunt gebruiken, maar ook wat er typisch mis gaat. Dat laatste kun je niet echt leren, dat is soms gewoon een beetje creatief nadenken over waar zou het fout kunnen gaan. Daar zijn geen regels voor, je kunt wel voorbeelden geven. Je hebt je eigen fantasie en creativiteit nodig om ergens gaten in te schieten.
Hoe leer je creatief nadenken? Hoe breng je dat over?
Je kunt voorbeelden noemen, je ziet daar wel terugkerende patronen in. Maar uiteindelijk kun je het niet echt leren.
Dus dan moeten ze daar maar zelf achter komen?
Ja.
Voor hardware en software zijn er standaard technieken die je kunt gebruiken (voor die eisen).
Waarom is het belangrijk dat ze die eisen leren?
Als mensen een systeem bouwen kijken ze in eerste instantie naar de functionaliteit en dan gaan ze hooguit achteraf pas nadenken over wat er allemaal mis kan gaan. Ik denk dat het belangrijk is dat als je het systeem neerzet dat je dan al denkt van wat zijn de risico's die je loopt en in dat stadium.
Dus eigenlijk van te voren als zorgen dat je een goed systeem bouwt?
Ja.
Hoe leer je wat over die eisen? Zeg je gewoon van dit zijn de eisen?
Je kunt met die eisen op heel hoog niveau beginnen, confidentialiteit, integriteit, authenticatie, je kan standaard nadenken over wat voor authenticatiemechanismen je gebruikt, hoe je bepaalde verbindingen beveiligd. Het grote probleem bij security is, je hoeft het maar ergens over het hoofd te zien en je hangt.
Wat voor opdrachten maak je over die eisen?
Bij hardware security laten we de studenten zelf een oplossing bouwen. Ze moeten een systeem ontwerpen, de security eisen formuleren, zelf protocollen maken om het te beveiligen en het uiteindelijk implementeren op een smartcard. Dat is dus vrij constructief en dan zie je ook dat mensen dingen over het hoofd zien bij het inventariseren van de security eisen. Iets klassieks wat je daar heel vaak ziet is dat iedereen er aan denkt om dingen te versleutelen maar bijvoorbeeld niet om een handtekening erop te zetten of een mac om de integriteit te waarborgen. Dat is opzich heel deterministisch dat mensen dat vergeten. We hebben dan bijvoorbeeld tien groepen die je een oplossing laat maken en dan kun je er de donder op zeggen dat zes vergeten dat eigenlijk integriteit veel belangrijker is dan confidentialiteit.
Dus door ze iets te laten bouwen toets je daarmee of ze die geleerde kennis uit het college begrijpen?
Ja, dan laat je ze iets bouwen en dan moeten ze het verantwoorden en dan geef je daar feedback op. En wij proberen er dan gaten in te schieten.
Hoe doe je dat, ga je gewoon alles uitproberen?
Nee niet echt je kijkt wel naar de standaard dingen die fout kunnen gaan. De helft van de groep gaat vergeten dat integriteit veel belangrijker is dan confidentialiteit.
Merk je ook dat ze bepaalde manieren van denken hebben dus van confidentialiteit is belangrijker dan integriteit en dan gaan ze allemaal daarop?

Ja, de eerste reflex van mensen is om dingen te gaan versleutelen terwijl dat eigenlijk helemaal niet belangrijk is. Dus daar zie je wel patronen in. Dat zie je wel bij security, dat mensen steeds dezelfde fouten maken. Dat heeft een voordeel, dan kun je er wat aan doen. Als iedereen de hele tijd iets anders fout doet, dan kun je er niks aan doen. Aan de andere kant is het frustrerend, dat moet je nu toch weten.
Het zijn telkens nieuwe studenten dus dan...
Ja dat is waar.
Zijn er ook dingen die bewust weglaat dus dingen die je ze niet wil leren?
Nee..
Dingen die jij wel weet maar dan niet aan bod komen in het college?
Nee in het college wil je alles aan bod laten komen.
Echt alle kennis die jij hebt over security?
Alle belangrijke issues wil je daar wel aan bod laten komen.
Is er geen heel klein onderwerpje, heel specifiek wat je achterwege laat?
Ja de brede thema's komen dan aan bod. Je kunt altijd meer voorbeelden of meer case-studies waarvan je dan toevallig meer weet, die kun je niet allemaal behandelen.
Die protocollen, geef je die ook in de les?
Ze hebben andere vakken gehad waarbij ze protocollen... ze hebben cryptovakken gehad. Er zijn vakken in de master waarbij ze protocolanalyse doen. Dit is andersom dan dat ze wat moeten ontwerpen.
En die protocollen zijn belangrijk omdat?
Daar hangt de hele security op.
Bij die protocollen komen ze dan nog problemen tegen. Wat je zei bij integriteit dat is een probleem bij de eisen, maar zijn er ook van die problemen bij protocollen?
Nee, je kunt bij protocollen.., in principe is dat een protocolprobleem als je integriteit vergeet te checken. Er zijn andere standaard protocolfouten van dat je er van die random getallen of nonces in moet gooien om replays te voorkomen. Moet je ook even aan denken.
Bij hardware gaan ze dus zo'n systeem bouwen en wat doe je bij software?
Bij software security, een deel is gewoon het beschrijven van standaard dingen die fout kunnen gaan in software want er zijn natuurlijk een hele hoop klassieke fouten: de bufferoverflows, de sql-injection, de cross-site scripting, dus dat soort dingen komen aan bod. En dan komen er wat technieken aan bod om daar tegen te beschermen en dan laat ik studenten ook een code-review doen voor een webapplicatie. Dus dat ze een webapplicatie moeten bekijken, om te zeggen, hoe veilig is die aan de hand van een soort richtlijnen voor zo'n review die er zijn gemaakt. Ook om ze even te confronteren met het probleem dat, ja, om voor een willekeurige applicatie, met duizenden regels code, ja hoe ga je dat...
En hoe beoordeel jij dan of ze dat goed hebben gedaan?
Ze moeten verantwoorden van waarop hun conclusie gebaseerd is.
En wanneer vind je dan dat ze een goede conclusie getrokken hebben?
Als ze daar goede argumentatie voor kunnen geven, ja weet ik, sql-injection, je kunt kijken van hebben ze de standaard dingen gedaan om een sql-injection te voorkomen. Dat is iets of, kun je een voorbeeld geven waar het mis gaat. Als ze dat niet hebben gedaan kunnen je misschien ook laten zien van dat je daar een gat door hebt.
Zijn er nog andere factoren die je onderwijs beïnvloeden, de tijd bijvoorbeeld of het materiaal? Ik kan me voorstellen dat er van security niet heel veel literatuur beschikbaar is, of valt dat mee?
ja soms is er weinig literatuur beschikbaar, of niet echt de geschikte literatuur.
En hoe los je dat dat op?
Wat ik probeer is om wetenschappelijke publicaties als literatuur aan te voeren, is ook leuk dat mensen dat eens een keer lezen. Of dat ik zelf stukken dictaat schrijf.
Volg je zeg maar de standaard structuur van je geeft college en daarna is er zelfstandig werken, of hoe zit dat in elkaar? Verschilt het nog bij de vakken?
Wat ik wel altijd probeer is dat mensen zelf ergens mee aan de slag gaan. Bij hardware security is dat een heel groot deel want ze moeten zelf zo'n hardware applicatie gaan zitten te ontwerpen, bouwen en implementeren. Bij software security zitten wel wat opdrachten waarbij ze met tools

aan de gang gaan.
Doen ze dat dan thuis allemaal of krijgen ze nog begeleiding om aan die opdracht te werken?
Meeste opdrachten zijn gewoon thuis en sommige opdrachten doen we dan wel eens dat het in een computerzaal is, dat je mensen kan helpen met praktische dingen.
Maar dat is niet standaard, geen standaard werkcollege ofzo?
Nee, bij de mastervakken heb je dat eigenlijk weinig. en ook ook omdat we met die Kerkhoffs master al onze vakken op een dag schedulen, dus dan gaat het wel heel moeilijk worden om daar nog...
Bij die webapplicatie dat ze moeten reviewen, gaan ze daar dan iets over schrijven of doen ze alleen de verantwoording?
Ze moeten daar wel iets over schrijven.
Dus ze leveren dat in en geven een presentatie?
Ik gebruik dan meestal een wiki waar ze dat dan moeten documenteren, omdat ik dan ook meteen daarin kan gaan zitten, dan kan ik feedback geven.
Oh dus nog een andere manier van beoordelen.
Ja dan kun je tussendoor nog wel wat feedback geven of wat hints erin hangen. En in het verleden hebben we dan wel gedaan dat ze op het einde een presentatie moeten geven. Maar soms merk je dan wel dat de groepen te groot worden, dat we teveel groepen hebben, dis dan weet ik niet of dat dit jaar nog haalbaar is. Als je 5 groepen hebt kun je zeggen van dan vertelt iedereen 10 minuutjes iets. Maar we hebben dit jaar 11 groepen, dan wordt het een beetje de vraag, van is dat nog te doen om te laten presenteren, want het wordt vaak ook ontzettend saai dan.
Dus dan doen ze die verantwoording ook alleen maar schriftelijk?
Nee, of dat je meetings hebt per groepje om even feedback te geven.
Is er dan ook nog een tentamen op het einde?
Bij software security wel, bij hardware security niet echt.
Dan heb je zeg maar alleen de beoordeling dat ding wat ze gemaakt hebben?
Ja dat project. ja en ze hebben dan nog wat kleinere opdrachten die ze ook met z'n tweeën of individueel doen.
Daar krijgen ze ook nog een cijfer voor?
Ja daar krijgen ze ook nog een cijfer voor en dat tellen we dan op en middelen we een beetje.
En bij software hebben ze dan die review en..?
Ja ze hebben dan drie projecten, twee individueel en een met de groep en een tentamen.
En dat tentamen, dan toets je vooral de kennis denk ik?
Ja dan ga je meer op de theoretische, meer op de kennisaspecten, niet de praktijkdingen.
En als je dan les geeft in een college, begin je dan eerst met een voorbeeldje of eerst met de algemene theorie?
Ja meestal, bijna altijd probeer je dingen aan voorbeelden op te hangen.
Je kan ook zeggen, ik doe eerst de theorie en dan geef ik voorbeelden.
Ja soms werkt het, maar meestal werkt het beter andersom, om eerst de voorbeelden te geven en dan de...
En wat vind je belangrijk dat mensen zich herinneren als ze zo'n vak hebben afgesloten?
Wat vind je belangrijk wat nou blijft hangen, of moeten ze alles onthouden?
Nee, ik kan me voorstellen dat je veel van die dingen niet onthoudt.
Of is het meer de ervaring?
Ja het deels ervaring. Als je mensen zelf zo'n protocol laat maken en het laat implementeren, dan ervaren mensen van hoe lastig dat is en hoe makkelijk het is om daarmee fouten te maken. Ja bij software security, ik hoop wel dat ze onthouden van, ja er zijn een heleboel van de programmeertaal en de soort applicatie die je maakt, zijn een hoop standaard valkuilen, van je moet dit niet doen, want dan gaat het daar mis. Opzich is het goed dat mensen dat beseffen en als ze later applicaties gaan maken in de praktijk in een bepaalde programmeertaal, dat ze ook actief opzoek gaan naar kennis van, hoe moet ik het in deze programmeertaal doen, om het goed te doen. Ik kan daar toch ook niet voor tien programmeertalen, van hoe doe je een veilige sql-query, dat je geen sql-injection hebt. Meer dat mensen beseffen van dit is een standaard probleem en dat ze dan gaan kijken hoe doe ik het in deze taal goed.

Ook zegmaar meer een soort houding die je ze wil aanleren?
ja maar het is dus heel specifiek de houding dat je opzoek moet gaan naar kennis, omdat er tegenwoordig opzich wel veel bekend is over die standaard manieren, waarom dingen fout gaan. En algemeen, maar dat is breder in security, wil meegeven is een bepaalde security mindset, dat je kritisch nadenkt over een ontwerp en daar probeert gaten in te schieten. Dat je typisch wilt, ja ,dat mensen naar hun applicatie kijken als een aanvaller en denken van ok, en wat zijn nou de dingen die ik zou willen aanvallen, hoe zou ik dat doen, en dat je op die manier nadenkt van heb ik op de goede plekken dingen goed beveiligd. En je zei al van dat creatief nadenken, dat wil je dus eigenlijk wel leren, maar dat is wel heel moeilijk.
Ja, zo'n mindset, dat is heel moeilijk om dat over te brengen. Toch vaak van, een heleboel van die standaard anekdotes: hier is het zus misgegaan, daar is het zo misgegaan. En uit die anekdotes zie je wel vaak van die patronen terugkomen van typisch die dingen die mensen fout doen. Maar het blijft lastig. je kunt niet een checklist maken met tien dingen van hier moet je je aan houden en dan gaat het goed.
Maar probeer je dan met die projecten niet al te stimuleren dat ze creatief nadenken, zelf?
Ja natuurlijk, dat probeer je dan te stimuleren.
En die projecten, mogen ze dan zelf een onderwerp bedenken, of hoe gaat dat, lever je die aan?
ja bij hardware security hebben we gewoon een paar standaard dingen die mensen kunnen implementeren, maak een soort chipknip-achtig iets of, een beetje variaties op hetzelfde thema, t komt allemaal op hetzelfde neer.
En bij software?
Bij sommige tooltjes dan hebben we gewoon standaard voorbeeldjes, want dan moet je het een beetje gecontroleerd houden, dat je het een beetje voorspelbaar hebt. Maar bijvoorbeeld bij zo'n code-review dan mogen ze ook zelf zeggen van, dit is een webapplicatie waar ik naar wil kijken.
En kijk je dan van te voren van, deze webapplicatie is geschikt, of zeg je van ga maar aan de slag?
Nou dan mogen ze opzich zelf kiezen.
Ja want ze leren dan natuurlijk ook heel veel over de webapplicatie, dus niet direct over security.
Ja maar wat je dan vooral leert is het probleem om zo'n applicatie te begrijpen. Hoe is het georganiseerd en waar is nagedacht over de security, waar is niet nagedacht over de security.
Kun je misschien nog een verschil noemen tussen hardware en software security wat heel opvallend is? Ja hardware gaat echt over de hardware, maar het is allebei security, dus... Die eisen blijven denk ik toch hetzelfde.
Veel dingen blijven toch hetzelfde. En ook het feit dat mensen zo'n protocol moeten maken, moeten implementeren, dat het dan op speciale hardware draait is wat dat betreft minder relevant.En dat vak gaat er ook wel overheen, specifieke hardware-aanvallen.
Maar als je zo'n hardware-project doet, dan ben je ook wel met software bezig.
Ja uiteindelijk is het software, alleen mensen moeten een smart-card-implementatie maken, dus we geven ze een smart-card en dan moeten ze daar de software op zetten. Dan merk je ook wel dat dat een redelijk obscuur en raar platform is om op te programmeren. Je moet heel voorzichtig programmeren, want je hebt heel weinig resources op je systeem, ja 256 bytes RAM, dat is anders dan de gemiddelde computer. Wat wel leuk is dat je ziet dat, het is heel laag niveau programmeren met bytes en bits enzo, dat doe je met normaal programmeren eigenlijk niet want dan trek je een paar van die bibliotheken open en dan ga je aan de slag. Opzich heeft dat niet zoveel met security te maken, maar wel met dit soort embedded hardware, is dat het debuggen afgrijselijk lastig is. Normaal als je een programma hebt en hij doet het niet dan zet je er een paar print-lines in, maar op een smart-card kan je er geen print-lines in zetten. Dat is opzich ook wel een beetje een bijkomende ervaring, dat mensen realiseren dat dat soort embedded dingen, dat dat best akelig programmeren is. Dus ook bijvoorbeeld dat je in Java normaal een nullpointer exception hebt, dan krijg je een nullpointer exception en stack trace, dan kun je precies zien waar die is. Op zo'n smartcard krijg je: error. Dan kun je gaan uitvogelen wat er dan mis was.
Ja dat is waar, dus ze leren eigenlijk ook wel debuggen.
Ja, maar dan leer je misschien ook dat je in zo'n omgeving veel gedisciplineerder aan het werk gaan met programmeren, want je kunt niet gewoon, wat je in feite doet, wat programmeren en dan zie je wel waar het fout gaat en dan een beetje bijsturen, want dat werkt daar helemaal niet.

Hoe zorg je dan dat ze dat gaan doen, zo gedisciplineerd programmeren?
Daar komen ze vanzelf achter, van shit dat is best wel lastig.
Ja dan moeten ze wel, want anders komen ze er niet uit.
Iets wat je ook merkt is, als je bijvoorbeeld met crypto werkt, dat dat ook ontzettend lastig is om te debuggen. Omdat de bedoeling van crypto is dat je helemaal geen informatie lekt. Maar dat betekent met debuggen dat als je een berichtje aan het decrypten bent, maar je hebt een offset net verkeerd, dan krijg je echt garbage terug. En dan kun je ook niet zien van ik ben een bit te ver.
Maar dan moet je echt weer die structuur...
Maar dan zie je als developer werkt crypto je tegen want als je ergens een key verkeerd hebt geïnstalleerd dan krijg je helemaal geen zinnige informatie terug.
Bij software gaat het dus veel makkelijker, het programmeren? Ja dan gaan ze ook iets bekijken.
Ja daar is meer het probleem dat die applicaties zo verrekte groot zijn. Zo'n smart-card-programmaatje is een paar honderd regels, dat kun je nog een beetje overzien, maar een gemiddelde webapplicatie dat wordt lastiger.
Zijn er ook dingen die je op verschillende manieren uit kan leggen? Een heel simpel voorbeeldje, het optellen van bits kan je uitleggen als een xor of je kan het uitleggen als optellen modulo 2.
Ik kan me voorstellen, bij security kan je het meer wiskundig uitleggen of meer praktisch, van zo moet het en doe maar gewoon, of dat je toch meer de achtergrond uitlegt.
Ik weet niet of er verschillende manieren zijn, je probeert dingen wel op verschillende niveaus uit te leggen. Vaak wil je dat mensen de intuïtie achter iets begrijpen. Als je bijvoorbeeld een of andere formelere methode hebt om iets te analyseren ofzo, dan wil je misschien die methode uitleggen dat mensen snappen hoe zoiets werkt, maar ook dat ze de intuïtie begrijpen van wat je er uiteindelijk mee bereikt. Dat is meer verschillende abstractie niveaus, dan verschillende manieren om het uit te leggen.
Begin je eerst met een hoog abstractieniveau en ga je dan omlaag of andersom of doe je het door elkaar heen?
Nou meestal begin je dan met voorbeelden om de intuïtie achter het probleem uit te leggen en daarna ga je dan misschien meer de diepte in. En misschien op het eind probeer je het nog even terug te koppelen, even weer de stap terug te maken, dat ze zien, van dat was het.

7.2 Tentamen Security

Exam Security

20 January 2011, 8:30 – 10:30

You can score a maximum of 100 points. Each question indicates how many points it is worth. You are NOT allowed to use a calculator. You may answer in Dutch or in English. Please write clearly, and don't forget to put your name and student number on each page.

1. To protect sensitive information on your computer you can use tools to encrypt your hard disk.

   (a) **(2 points)** Should these tools use symmetric key or public key encryption? Briefly explain your answer.

   (b) **(4 points)** The benefit of full disk encryption is that it encrypts all data on your disk. This is, however, also a drawback of such encryption tools. Explain why.
   (Hint: compare this to single file encryption.)

   (c) **(8 points)** When the computer is started it needs the decryption key to decrypt the disk and start the operating system. The strength of such tools depends much on how the key is protected. For each of the following methods classify

   - the kind of authentication of the user, and
   - the level of protection of the key (use for example high, medium, low)

   they provide and briefly explain your answers.

   i. Using a smart card in combination with a PIN.
   ii. Using a biometric authentication method such as a fingerprint.
   iii. Using a USB-stick to store the key.
   iv. Using a boot-time driver that can ask for a password from the user.

   (d) **(6 points)** An alternative to full disk encryption is to encrypt only a single (user) partition, which you will use to store your sensitive information, while everything else remains unencrypted. Another option is to encrypt each sensitive file separately. Give at least one benefit and one drawback for each of these two alternatives.
   (Hint: think about the difference when you have little or much sensitive information.)

2. Consider the following two messages.

   i. $A \longrightarrow B : m, K_{AB}\{h(m)\}$
   ii. $A \longrightarrow B : m, [h(m)]_{d_A}$

   where K_{AB} is a secret key shared between A and B, d_A is the private key of A, and h is a secure hash function.

   (a) **(10 points)** List the security goals that are achieved by each of these two messages.

   (b) **(10 points)** If a goal is achieved by one message, but not by the other, explain why.

3. In the context of RSA consider the two primes $p = 3$ and $q = 5$. Give intermediate steps for all your computations, together with an explanation, if needed.

   (a) **(6 points)** Which public keys are possible? List them all, and compute the corresponding private keys.

   (b) **(6 points)** Suppose in this context Alice has public key $e = 3$, and you wish to send here confidentially the message $m = 7$. Calculate which value you should send her.

   (c) **(6 points)** Now suppose you want Alice to blindly sign the message $m = 7$. Compute the blinded message $m' = m \cdot r^e$, using random value $r = 2$, that will be sent to Alice.

(d) **(6 points)** Explain how to do a blind signature on m and perform the necessary computations, using the blinded message m' and random $r = 2$ from the previous question.

(e) **(6 points)** Verify that these steps indeed give you a valid signature of Alice on the message $m = 7$.

4. Consider the following (simplified) RFID authentication protocols from the literature. In both protocols, the reader R holds a list of pairs $(\text{tagid}_1, k_1) \ldots (\text{tagid}_n, k_n)$ that he uses to authenticate a tag. The tag T holds its tag identifier tagid and its secret key k shared between tag and reader. After running an authentication protocol, the reader iterates over his entire list until he finds a matching pair (tagid_i, k_i) and in this way he authenticates the tag. Notation: The symbol $\oplus$ denotes the 'exclusive or' operation (XOR), n_1 and n_2 are nonces and h is a secure hash function.

Protocol 1

$R \longrightarrow T : n_1$

$T \longrightarrow R : n_2, h(n_1 \oplus n_2 \oplus k)$

Protocol 2

$R \longrightarrow T : n_1$

$T \longrightarrow R : \text{tagid} \oplus n_2, h(n_1, k) \oplus n_2$

Both protocols are claimed to achieve the following security goals:

- tag authentication
- location privacy (this means that an attacker that talks with a tag cannot, latter on, even recognize if he is talking with the same tag (and thus trace it))

but this is not true. Protocol 1 does not achieve tag authentication and Protocol 2 does not achieve location privacy.

(a) **(7 points)** For Protocol 1, give an attack that breaks tag authentication. Use notation like $R \longrightarrow T : m$.
(Hint: the attacker plays as eavesdropper/tag.)

(b) **(7 points)** For Protocol 2, give an attack that breaks location privacy. Use notation like $R \longrightarrow T : m$.
(Hint: the attacker plays as reader.)

(c) **(8 points)** Fix each protocol by modifying only one message, in such a way that both goals are achieved. Explain your fix.

(d) **(8 points)** Explain which of the following properties of the hash function h are necessary to achieve location privacy for Protocol 1 and tag authentication for Protocol 2.

(E) h can be computed efficiently,

(O1) given a bit string y it is infeasible to determine a bit string x such that $h(x) = y$ (pre-image resistance),

(O2) given a bit string x it is infeasible to determine a different bit string x' $(x \neq x')$ such that $h(x) = h(x')$ (2nd pre-image resistance),

(C) it is infeasible to determine any two different bit strings x and x' $(x \neq x')$ such that $h(x) = h(x')$ (collision resistance).

7.3 De module

Module

Cybersecurity

Uitgegeven op 11 juli 2013

Ontwikkeld door:
Petra van den Bos

Onder begeleiding van:
Erik Poll
Marko van Eekelen

Radboud Universiteit

Inhoudsopgave

1 Inleiding cybersecurity

1.1 Wat is cybersecurity?

Cybersecurity gaat over het beveiligen van **digitale informatie** en **digitale diensten** die een bepaalde waarde hebben. Die waarde zorgt ervoor dat je de informatie of dienst wilt afschermen. Bij digitale informatie kun je bijvoorbeeld denken aan cijfers of medische gegevens. Bij digitale diensten kun je denken aan internetbankieren, Gmail en Facebook. Het 'cyber' in cybersecurity benadrukt extra dat het gaat om security in de digitale wereld.

Digitale informatie wordt meestal beschermd met behulp van cryptografie. Meer hierover volgt in de hoofdstukken 'Symmetrische cryptografie' en 'Asymmetrische cryptografie'.

Bij digitale diensten is het vaak van belang om alleen bepaalde mensen toegang te geven tot de dienst waarvan jij gebruik maakt. Meestal heb je zelf toegang. Soms horen er ook mensen bij die je vertrouwt, zoals bijvoorbeeld iemand waarmee je je internetrekening deelt. Belangrijk is dus dat er controle is over de toegang: **toegangscontrole**. Een voorbeeld van toegangscontrole is als een website controleert of jouw username en wachtwoord kloppen. Toegangscontrole wordt uitgebreider behandeld in het hoofdstuk 'Identiteit en authenticatie'.

Figuur 1: Toegangscontrole
http://whitestarflower.deviantart.com/art/Airport-Metal-Detector-185600324

De beveiliging van de digitale informatie en diensten kan door een ongelukje geschonden worden, maar ook doordat iemand met kwade bedoelingen actief heeft gezocht naar een gat in de beveiliging. Zo iemand met kwade bedoelingen noemen we een **aanvaller**. In de security gaan we altijd uit van het ergste geval, dus dat er altijd zo'n aanvaller is. Ook gaan we ervan uit dat de aanvaller over alle kwaliteiten en hulpmiddelen beschikt. Een aanvaller is dus gemotiveerd, intelligent, creatief, geduldig enz. en heeft beschikking over de beste apparatuur. Het veronderstellen van zo'n actieve aanvaller is precies het verschil met **veiligheid**, daarbij wordt alleen gezorgd voor bescherming tegen ongelukken en fouten.

Opdracht 1: Indringer

Zoek een nieuwsbericht waarbij het gelukt is om om de digitale beveiliging van een bedrijf heen te komen.

(a) Wie was of waren (vermoedelijk) de aanvaller(s)?

(b) Om welke digitale informatie ging het? Het hoeft niet zo te zijn dat er informatie is uitgelekt, misschien werd de informatievoorziening juist wel geblokkeerd, of is er niks met de informatie gedaan, maar was de informatie wel beschikbaar voor de aanvaller(s).

(c) Wat was er mis met de beveiliging waardoor de toegangscontrole niet werkte?

(d) Had deze aanval voorkomen kunnen worden? Hoe dan?

1.2 Communicatie

Als wij mensen toegang willen hebben tot digitale informatie of diensten, communiceren we met het apparaat waar die informatie op staat om die informatie te verkrijgen of communiceren we met het apparaat waar die dienst ter beschikking wordt gesteld. Je kan niet direct aan het apparaat zien wat hij heeft opgeslagen. Alle soorten **communicatie** kun je zien als het versturen van berichten. Op een computer klik je bijvoorbeeld een bestand aan om het te openen. Dit klikken is dus al communicatie. Je zegt tegen de computer dat hij het bestand moet openen, dus de inhoud van het bericht is de vraag om het bestand te openen. Het concept **bericht** vatten we dus heel breed op.

Ook als mensen met elkaar communiceren sturen ze elkaar berichten, bijvoorbeeld door met elkaar te praten of gebaren te gebruiken. Als er een apparaat tussen zit typ je meestal een bericht, bijvoorbeeld een e-mail of sms. Maar je kunt ook bellen of skypen.

Elk bericht heeft een inhoud, een zender, één of meerdere ontvangers en een **medium** waar het bericht over gestuurd wordt. Het medium maakt het mogelijk dat het bericht van de zender naar de ontvanger gaat. Voorbeelden van media zijn gsm (communicatie tussen mobiele telefoons), internet over kabel en wifi (draadloos internet). Als je tegen iemand praat ben jij de zender, zijn de toehoorders de ontvangers, is wat je zegt de inhoud van het bericht en is de lucht het medium, want daar gaat het geluid van je stem doorheen voordat het de ontvangers bereikt.

Figuur 2: Een bericht
http://1ms.net/the-message-233530.html

Soms zijn er ook onbedoelde ontvangers van het bericht, iemand die stiekem meeluistert. Of zelfs iemand die je bericht aanpast voordat het bij de ontvangers aan komt. Als je met elkaar praat kan iemand het aanpassen door er hard door heen te schreeuwen zodat je elkaar niet verstaat. Maar echt het bericht een andere inhoud geven lukt niet als je met elkaar praat, maar kan wel in de digitale wereld.

Om uit elkaar te houden wie goed en wie kwade bedoelingen wordt er in de security vaak gesproken over bepaalde personages. Alice en Bob zijn de ‘good guys’. Zij sturen elkaar berichten.

Eve (van 'evil') is de slechterik. Zij probeert Alice en Bob op alle mogelijke manieren dwars te zitten. Vaak worden alleen de initialen A, B en E gebruikt om Alice, Bob en Eve aan te duiden. Voortaan zullen deze personages ook hier gebruikt worden.

Je kunt meer lezen over Alice, Bob en Eve op: http://downlode.org/Etext/alicebob.html.

Opdracht 2: Flessenpost

(a) Wat zijn de inhoud, de zender, de ontvanger(s) en het medium van het bericht in figuur 2?

(b) Verzin zelf een voorbeeld van een bericht en geef aan wat de inhoud, zender, ontvanger(s) en medium van dit bericht zijn.

1.3 Security Doelen

Voor het kiezen van de juiste soort beveiliging is het van belang te weten wat je wilt bereiken met de beveiliging. Daarom volgen hier een aantal algemene doelen. Ieder praktijkvoorbeeld kun je indelen bij één of meer van deze doelen. In de security worden de doelen vaak met het Engelse woord aangeduid.

- **Vertrouwelijkheid** (Confidentiality): Eve kan niet lezen wat de inhoud is van de berichten die Alice en Bob naar elkaar sturen.

  Van sommige gegevens willen we niet dat iedereen er zomaar toegang tot heeft: we willen dat deze digitale informatie vertrouwelijk blijft. Denk bijvoorbeeld aan medische gegevens, geheime staatsinformatie, militaire informatie, in-formatie die de politie heeft over verdachten en criminelen, maar ook informatie die criminelen hebben en waarvan ze niet willen dat de politie of concurrerende criminelen er achter komen. In het bedrijfsleven is er ook veel vertrouwelijke informatie, bijvoorbeeld klantgegevens, of andere informatie die interessant kan zijn voor concurrenten. Zelf heb je ook de nodige gegevens die vertrouwelijkheid is: denk maar je pincode of je wachtwoord, al je sms'jes en e-mails, en alle skype-berichten die misschien ergens in een log bestand worden bijgehouden.

  Privacy is een bijzonder geval van vertrouwelijkheid, en wordt gebruikt als het over de vertrouwelijkheid van privégegevens gaat. Denk bijvoorbeeld aan medische gegevens, financile gegevens van hoeveel geld iemand op zijn bankrekening heeft, maar ook aan de cijferadministratie op school, waarvan het niet de bedoeling is dat iedereen mag inzien welke punten jij hebt gehaald. Hier gelden ook speciale wettelijke regels voor.. Privacy zelf zal besproken worden in het hoofdstuk 'Privacy'.

- **Integriteit** (Integrity): Eve kan de inhoud van de berichten die Alice en Bob naar elkaar versturen niet veranderen.

  Behalve dat we van sommige gegevens niet willen dat iedereen ze kan lezen, willen we al helemaal niet dat iedereen ze zou kunnen veranderen. Dit is van belang om informatie te kunnen vertrouwen. We zeggen dan dat de integriteit, oftewel de echtheid, van deze informatie van belang is.

  Voor informatie waarvoor vertrouwelijkheid van belang is, is integriteit dat vaak ook. Je wilt niet dat iedereen je medische gegevens kan lezen, maar al helemaal niet dat iedereen ze zou kunnen veranderen! Als verkeerde informatie over iemands bloedgroep, of allergiën voor antibiotica, in dossiers terecht komt veranderen kan grote problemen veroorzaken. Het wijzigen van je eigen financiële gegevens bijvoorbeeld hoeveel geld er op je bankrekening staat zou erg interessant zijn, maar de bank wil dat natuurlijk voorkomen: voor de bank is integriteit van deze informatie van essentieel belang.

- **Beschikbaarheid** (Availability): Eve kan niet voorkomen dat Alice en Bob met elkaar communiceren.

Sommige computeraanvallen hebben als enige doel om een computersysteem, bijvoorbeeld een website, plat te leggen. Dit heten DoS (Denial-of-Service) aanvallen, en we zullen ze uitgebreider bespreken in het hoofdstuk 'Digitale gevaren'.

De beveiligingseis die hiermee gebroken wordt is de beschikbaarheid van die website. Beschikbaarheid is een hele fundamentele beveiligingseis voor veel systemen. Hij ligt vaak zo voor de hand dat we er niet aan denken.

In de digitale wereld is beschikbaarheid vaak moeilijk te garanderen, en veel moeilijker dan we in de fysieke wereld gewend zijn. Bijvoorbeeld, je kunt een Denial-of-Service aanval op een warenhuis in de stad uitvoeren door met tienduizend mensen de winkel binnen te lopen, zodat iedereen hopeloos klem komt te staan en ook de echte klanten met geen mogelijkheid naar binnen kunnen, of, als ze al binnen zijn, niet bij de kassa kunnen komen. Dat is niet zo eenvoudig, want je moet erg veel mensen op de been brengen. Op internet gaat zoiets veel makkelijker! Je hebt helemaal geen echte mensen hiervoor nodig, want je kunt de boel automatiseren, en met computerprogrammas duizenden virtuele klanten een webwinkel binnen laten gaan om de boel vast te laten lopen.

- **Authenticatie** (Authentication): Alice weet zeker dat ze met Bob communiceert en niet met Eve.

  Authenticatie zorgt er dus voor dat je zeker weet met wie je communiceert. In het dagelijks leven gaan we daar nogal relaxed mee om. Je ID of paspoort gebruik je nauwelijks, de meeste mensen met wie je iets te maken hebt ken je eigenlijk wel en anders vraag je het aan een 'tussenpersoon'. Toch zijn er wel regels. Als een agent om je ID vraagt heb jij het recht om die agent te vragen zich eerst zelf te identificeren. Het kan tenslotte wel carnaval zijn, waardoor de persoon voor je alleen verkleed is als agent en geen echte agent is. Als de agent weigert, mag jij ook weigeren.

  Als je in het ziekenhuis een man ziet in een witte jas, wat denk je dan? Dat zal wel een docter zijn. En als je een vrouw ziet in een witte jas? Dat zal wel een verpleegster zijn. Misschien verrassend is dan om te weten dat er meer vrouwelijke specialisten zijn!

  Authenticatie is niet alleen belangrijk bij personen. Neem bijvoorbeeld een pinautomaat. Je toetst daarop zomaar je pincode in, hoe weet je nou dat het geen nep-automaat is? In een winkel ga je ervan uit dat het wel in orde zal zijn, maar op een autosloop moet je misschien iets voorzichtiger zijn...

  In het dagelijks leven vertrouwen we dus erg op informatie uit de omgeving: **context**. Context is dus bijvoorbeeld het uniform van de agent die suggereert dat je met een agent te maken hebt, het ziekenhuis en de witte jas die suggereert dat je met ziekenhuispersoneel te maken hebt en het bankgebouw in een drukke winkelstraat die suggereert dat je met een pinautomaat te maken hebt.

  In de digitale wereld ontbreekt die context vaak en is iets ook makkelijker te vervalsen. Een bankgebouw namaken is een gedoe en ook erg zichtbaar, maar even een website opzetten om te kunnen internetbankieren is veel makkelijker en wordt niet direct opgemerkt. In hoofdstuk 'Identiteit en authenticatie' volgt meer.

- **Onweerlegbaarheid** (Non-repudiation): Alice en Bob kunnen niet ontkennen wat ze gecommuniceerd hebben.

  Als iemand je iets laat ondertekenen, kun je later niet meer ontkennen dat je ermee akkoord bent begaan. Dit betekent dat het contract onweerlegbaar of onontkenbaar is. Onweerlegbaarheid is een belangrijke eigenschap in veel systemen. Maar hoe regel je onweerlegbaarheid in de digitale wereld?

  Als onenigheid over een contract ontstaat, kan iemand zelfs naar de rechter stappen. Net zoals er wetgeving is over het gebruik van handtekeningen, zal er ook wetgeving nodig zijn voor de tegenhangers van handtekeningen in de digitale wereld. Een belangrijke manier

Figuur 3: Contract
http://nl.123rf.com/photo_10959836_ondertekening-contract-met-vulpen-icoon.html

om onweerlegbaarheid te realiseren is het gebruik van digitale handtekeningen, en hier is inderdaad ook de nodige wetgeving over.

Handtekeningen zijn niet de enige manier om onweerlegbaarheid te realiseren. Als je ergens mondeling mee akkoord gaat is dit ook bindend, al is het moeilijker dit af te laten dwingen door een rechter, tenzij er getuigen zijn.

In de digitale wereld zie ook allerlei manieren om onweerlegbaarheid te realiseren. Op websites moet je soms aanvinken dat je akkoord gaat met de gebruiksvoorwaarden voor je naar een volgende schermpje verder kan. Hiermee kan het bedrijf achter deze website hard maken dat je met deze voorwaarden akkoord bent gegaan.

Op software die je koopt zit soms een sticker die zegt dat je door het openmaken van de verpakking aangeeft dat je akkoord gaat met bepaalde gebruiksvoorwaarden. Dit is vergelijkbaar met het aanvinken hierboven, maar dan in de fysieke wereld in plaats van de digitale wereld. Of dit een goede manier is te zorgen dat kopers ergens mee akkoord gaan valt te twisten.

Bij alle manieren om onweerlegbaarheid te garanderen kan er uiteindelijk een rechter aan te pas komen, om af te dwingen dat iemand zich ergens aan houdt (door boetes), maar alleen als de rechter vindt dat deze manier wel betrouwbaar is.

Opdracht 3: Cijferadministratie

Welke security doelen zijn van belang bij de cijferadministratie op school? Denk hierbij niet alleen aan de centrale opslag van alle punten, maar ook aan het aanleveren van deze gegevens door docenten, en ook het maken van de rapporten die de leerlingen thuis aan hun ouders moeten laten zien.

Opdracht 4: Welk security doel?

Welk security doel wordt geschaad in de volgende gevallen? Kies het doel dat het meest van toepassing is. Leg kort uit waarom.

(a) Een politieagent drinkt een kopje koffie in een café. Daardoor hoort hij niet dat hij opgeroepen wordt via de radio in zijn auto.

(b) Je wordt gebeld. De man aan de telefoon zegt dat hij een ICT-medewerker van de ING is en dat er een grote storing is. Jouw internetbankier-account kan alleen herstelt worden met jouw inlognaam en wachtwoord. Natuurlijk wil je je geld terug, dus geef je je gegevens. Een dag later log je zelf in en zie je dat al je geld is weggesluisd naar een obscure rekening.

(c) Stel je hebt een app op je smartphone die al je GPS-gegevens doorstuurt. Daardoor kan de maker van de app precies zien waar je bent.

(d) Een look-a-like haalt steelt jouw ID op. Vervolgens fietst hij zonder licht. Hij wordt aangehouden en laat jouw ID zien aan de agent. Hierdoor krijg jij een boete thuisgestuurd.

(e) Een look-a-like 'leent' jouw ID zonder dat je het merkt. Hij maakt je ID na en bezorgd hem zonder dat jij het merkt weer aan je terug.

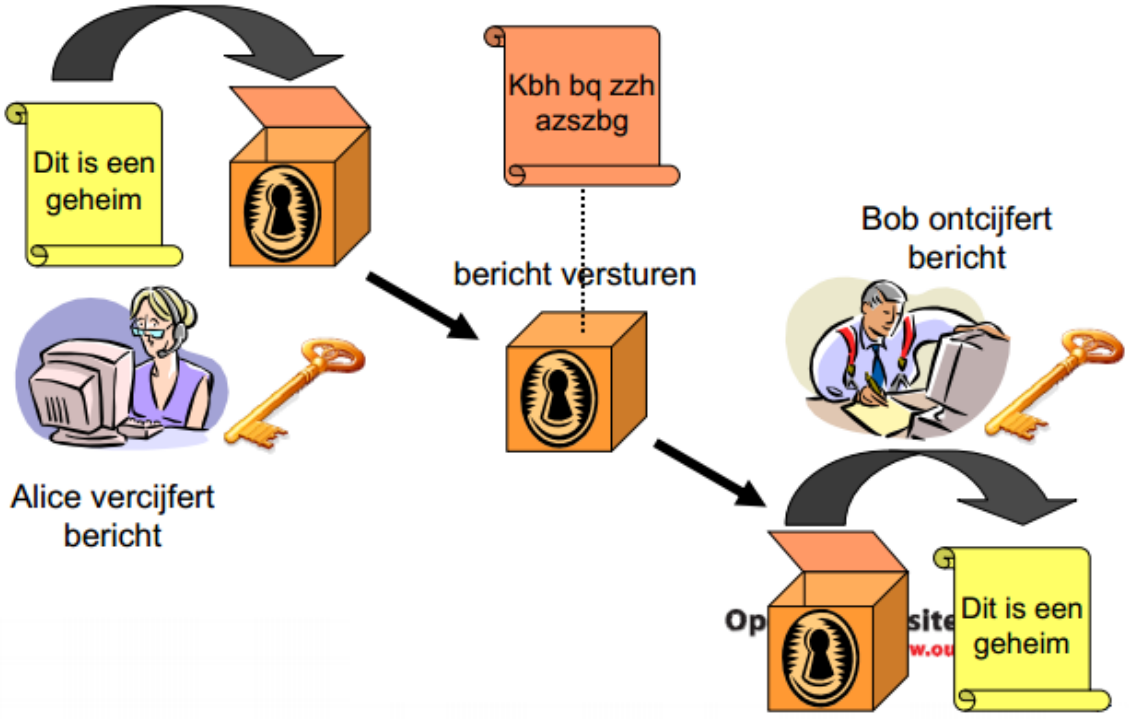
(f) Een look-a-like leest stiekem de vingerafdrukken op jouw ID uit.

(g) Het lukt een dief om de beveiligingsonderdelen, die op een kledingstuk zijn vastgemaakt, eraf te krijgen. Vervolgens loopt de dief zonder dat het alarm afgaat met het kledingstuk de winkel uit.

2 Symmetrische cryptografie

2.1 Geheime berichten

In het hoofdstuk 'Inleiding cybersecurity' heb je geleerd dat een van de doelen van security vertrouwelijkheid is. We willen niet altijd dat iedereen zomaar berichten kan lezen. Zo'n bericht moet geheim blijven. **Cryptografie** maakt dit mogelijk. Een cryptografische methode zorgt ervoor dat je een bericht onleesbaar kan maken en daarna ook weer leesbaar. Het onleesbaar maken noemen we **vercijferen** of **versleutelen** en het weer leesbaar maken **ontcijferen** of **ontsleutelen**. Hierbij is 'cijfer' een (slechte) vertaling van het Engelse 'cipher'. Een betere vertaling van 'cipher' is 'geheimschrift'. Een aantal cryptografische methodes zullen in dit hoofdstuk en in het hoofdstuk 'Asymmetrische Cryptografie' aan bod komen.



Figuur 4: Een geheim bericht versturen

2.2 Scytale

De Oude Grieken verstuurden al geheime berichten, bijvoorbeeld met de scytale. Dat is een cilinderstuk vormig hout. Om een bericht te vercijferen rolde je een lange strook papier om de scytale. Vervolgens schreef je van links naar rechts je boodschap op, waardoor op de strook dus telkens een stuk wordt overgeslagen. Daardoor staan de letters op de strook dus door elkaar. Vervolgens werd de strook naar de ontvanger gebracht. Die rolde de strook om een scytale met dezelfde diameter, waardoor hij het bericht van links naar rechts weer kon lezen. Als de ontvanger een scytale met een andere diameter zou gebruiken, ziet hij de letters door elkaar gehusseld. De ontvanger heeft dus een scytale met precies dezelfde diameter nodig als de ontvanger.

De strook kon door een willekeurige boodschapper vervoerd worden, want de strook bevatte geen leesbaar bericht. In de security gaan we er altijd van uit dat iedereen het bericht kan zien als

Figuur 5: Scytale

hij over het medium verstuurd wordt. We gaan er dus vanuit dat elk medium openbaar is. Als een medium niet openbaar is kan een aanvaller meestal wat apparatuur gebruiken om de communicatie toch af te luisteren. Bij de scytale is de boodschapper die het bericht over de wereld vervoert dus het medium.

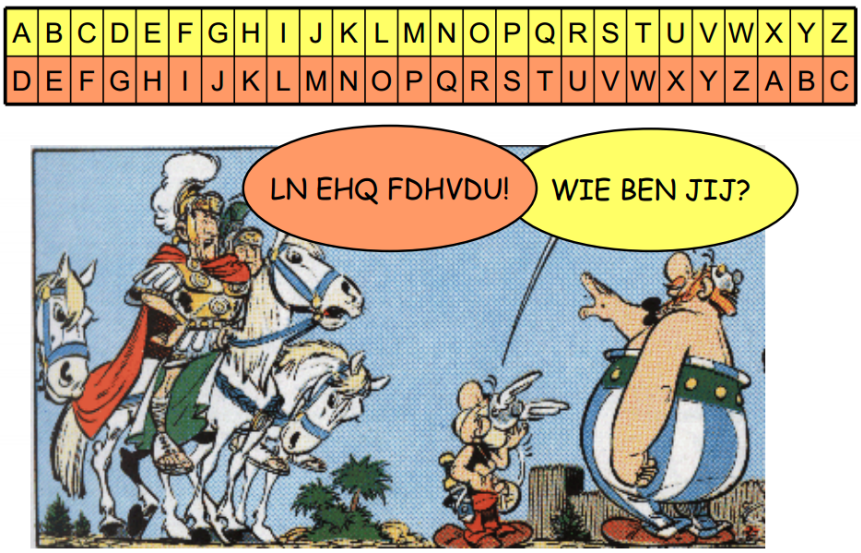
De strook is niet direct leesbaar, maar je kunt je vast voorstellen dat je met wat proberen er misschien wel zonder scytale achter kunt komen wat het oorspronkelijke bericht was. Dit maakt dat de scytale niet zo'n veilige methode is om berichten geheim te houden.

2.3 Ceasarcijfer

Ook de Romeinen maakten gebruik van cryptografie. **Caesarversleuteling** is een methode die zelfs door Caesar zou zijn gebruikt. Om een bericht te vercijferen verschuif je elke letter een aantal plaatsen naar rechts in het alfabet. Stel dat je elke letter drie plaatsen verschuift, dan wordt de A een D, de B een E, de C een F enzovoort. Omdat de W naar de Z vertaalt wordt, en Z de laatste letter is in het alfabet, beginnen we weer bij het begin van het alfabet. De X wordt dus een A, de Y een B en de Z een C. Op deze manier kan iedere letter vertaald worden.

Om het bericht te ontcijferen verplaats je alle letters evenveel plekken naar links. Voor het vercijferen en ontcijferen moet je dus weten hoeveel plekken elke letter verschoven is. Het aantal plekken is de **sleutel**. Zowel de zender als ontvanger gebruiken dezelfde sleutel om het bericht te vercijferen of te ontcijferen. Dat de zender en ontvanger dezelfde sleutel hebben is het kenmerk van **symmetrische cryptografie**. Met 'symmetrisch' wordt dus het hebben van dezelfde sleutel aangeduid.

Het verschuiven bij de ceasarversleuteling is de methode om een bericht te vercijferen en te ontcijferen, dit noemen we het **algoritme**. Het algoritme is dus altijd hetzelfde, de sleutel kan iedere keer anders zijn. Dit maakt ook dat het niet slim is om de geheimhouding van berichten te laten afhangen van de geheimhouding van het algoritme. Als het algoritme dan één keer uitlekt, zou je de berichten die in het verleden gestuurd zijn allemaal kunnen lezen. We gingen er namelijk van uit dat een bericht over een openbaar medium verstuurd wordt. Daardoor kun je alle verstuurde berichten opslaan, ook al kon je ze toen nog niet lezen. Voordeel van het algoritme openbaar maken is dat iemand misschien wel een foutje vindt, waardoor het algoritme verbeterd kan worden. Dat de geheimhouding van berichten niet mag afhangen van de geheimhouding van algoritme, alleen van de geheimhouding van de sleutel. Dit wordt het **het principe van Kerckhoffs** genoemd, omdat Auguste Kerckhoffs dit principe bekend maakte. Bij een website waarop je moet inloggen mag je dus best weten dat je alleen binnenkomt als je een loginnaam en bijbehorend wachtwoord



Figuur 6: Caesarversleuteling

hebt. Maar het wachtwoord is geheim.

2.4 Symmetrische cryptografie

Bij **symmetrische cryptografie** hebben de zender en de ontvanger dezelfde sleutel. Dit betekent dus dat alleen de zender en de ontvanger berichten die ze elkaar sturen kunnen vercijferen en ontcijferen. Als de zender een bericht naar meerdere ontvangers wil sturen moet de zender met iedere ontvanger een andere sleutel delen, want het is niet de bedoeling dat twee ontvangers ook berichten kunnen lezen die niet voor de een maar wel voor de ander bedoeld waren.

Behalve vertrouwelijkheid kun je met cryptografie ook andere security doelen bereiken. Als een bericht onleesbaar is, kun je er wel iets aan veranderen, waarmee je de integriteit van een bericht schaadt, maar je weet dan niet wat je verandert. De ontvanger merkt dan gelijk dat er iets mis is met het bericht als hij het ontcijfert, want het bericht bevat dan een stuk wat niet leesbaar. Dit komt doordat de aanvaller de sleutel niet heeft, waardoor hij zelf geen leesbaar stuk tekst kan vercijferen. Hij zou kunnen proberen te gokken, maar bij een veilige cryptografiemethode is er een verwaarloosbaar kleine kans op een leesbaar stuk tekst na ontcijferen van het gegokt stuk tekst.

Niet alle methodes om een bericht te vercijferen en ontcijferen zijn veilig. Als een methode onveilig is kun je een vercijfert bericht zonder sleutel ontcijferen. Als dit kan zeggen we ook wel dat je het bericht kan **kraken**. Soms is de methode onveilig omdat je met de hand het bericht al kan kraken, zoals met de scytale en caesarversleuteling. Soms is de methode onveilig omdat je met een snelle computer het bericht kan kraken. Een algemene methode om een bericht te kraken is de **brute force aanval**. Daarbij probeer je alle mogelijke sleutels uit en kijk je welke sleutel een leesbaar bericht oplevert. Bij de caesarversleuteling is een brute force aanval dus het proberen van alle mogelijke aantallen verschuivingen.

Het alfabet bevat 26 letters, dus zijn er 26 mogelijke verschuivingen. Als je elke letter 26 plaatsen verschuift, krijg je weer dezelfde letter, want dan ga je precies een rondje. Het bericht is na deze 'vercijfering' nog steeds leesbaar. Zo'n sleutel noemen we **triviaal** omdat het vercijferde bericht gelijk is aan het originele bericht. Zo'n triviale sleutel komt ook vaak bij andere cijfers voor. Als je een sleutel kiest moet je dus altijd controleren of het geen triviale sleutel is.

Als een aanvaller eenmaal een sleutel achterhaald heeft gaan we er in de security van uit dat hij alle berichten kan lezen die met die sleutel vercijferd waren en in het verleden verstuurd zijn. We

gingen er namelijk van uit dat een bericht over een openbaar medium verstuurd wordt. Daardoor kan de aanvaller alle berichten opslaan, ook al kon hij ze toen nog niet lezen. Nu hij de sleutel heeft kan hij alle berichten ontcijferen.

Opdracht 5: Scytale

(a) Wat is de sleutel van de scytale?

(b) Wat is het algoritme van de scytale?

(c) Heeft de scytale triviale sleutels?

(d) Gebruik twee keukenrollen en (aan elkaar geplakte) stroken papier om je buurman een geheim bericht te sturen.

(e) Probeer nu zonder keukenrol het bericht van je buurman te ontcijferen. Gebruik dat je al weet wat de eerste letters van het bericht zijn. Beschrijf hoe je dit gedaan hebt.

(f) Had je het bericht van je buurman ook kunnen ontcijferen zonder dat je wist wat de eerste letters waren?

2.5 Substitutie en transpositie

De scytale en ceasarversleuteling zijn niet de enige versleutelingsmethodes. De **substitutieversleuteling** bijvoorbeeld. Elke letter van het oorspronkelijke bericht wordt dan vertaalt naar een andere letter. De letters die een vertaling zijn van de oorspronkelijke letters zijn allen verschillend. Anders kun je het vercijferde bericht niet terugvertalen. Stel dat C wordt vertaald naar A en B ook naar A. Als er dan een A in het vercijferde bericht staat weet je niet of dat een B of C was in het oorspronkelijke bericht. Doordat alle vertaalde letters verschillend zijn, vormen de vertaalde letters samen weer het alfabet. Al is het niet noodzakelijk om als vertaling de letters uit het alfabet te nemen, dit kunnen ook andere symbolen zijn. De sleutel is dus een lijst met iedere letter uit het alfabet en zijn vertaling.

De caesarversleuteling is ook een substitutieversleuteling. Daar vertaal je ook iedere letter naar een (verschillende) letter. Bij een caesarversleuteling staan de vertalingen van twee opvolgende letters van het alfabet ook na elkaar in het alfabet. Bij de substitutieversleuteling hoeft dat niet, je mag best A naar C vertalen en B naar Q, zolang de vertaalde letters maar verschillend zijn.

Bij een **transpositieversleuteling** verander je niet de letters, maar de positie ofwel plaats van de letters. Je hutselt de letters van een bericht dus door elkaar. Dit moet je wel systematisch doen, anders kun je het oorspronkelijke bericht niet achterhalen uit het vercijferde bericht. Hiervoor delen we het bericht eerst in een aantal blokken met ieder hetzelfde aantal letters. Als er op het einde niet genoeg letters over zijn, zet je er wat willekeurige letters achter. Vervolgens vertaal je iedere positie in een blok naar een andere positie. De letter op de eerste positie gaat bijvoorbeeld naar de derde positie, de letter op de vierde positie naar de eerste enzovoort. De letters van elk blok wordt dus op dezelfde manier door elkaar gehutseld. De nieuwe blokken plak je gewoon weer achter elkaar.

Om het bericht weer te ontcijferen deel je het bericht eerst op in blokken. Daarna vertaal je alle posities terug naar de oorspronkelijke positie. Als bij het vercijferen een letter van de eerste naar de derde positie verplaatst werd, wordt een letter op de derde positie nu naar de eerste positie verplaatst.

Bij een transpositieversleuteling blijven de letters dus hetzelfde maar worden de posities van de letters veranderd. Bij een substitutieversleuteling blijven de letters op dezelfde positie staan, maar worden in een andere letter veranderd. Dit verschil maakt dat je door te tellen onderscheidt kan maken tussen een transpositieversleuteling en een substitutieversleuteling. Omdat de letters in een transpositieversleuteling hetzelfde blijven, komt elke letter nog even vaak voor in het vercijferde bericht als in het originele bericht. Het originele bericht is geschreven in een bepaalde taal. In een taal komen bepaalde letters vaker voor dan andere. In het Nederlands komt bijvoorbeeld

de e vaak voor en de q heel weinig. Hierdoor komt de e ook veel voor in de vercijferde tekst van een transpositieversleuteling en de q weinig. In een substitutieversleuteling verander je de letters, waardoor er opeens andere letters vaak en weinig voorkomen. De **letterfrequentie** van een letter geeft aan hoeveel procent van een tekst gemiddeld die letter is. Dus hoe groter de letterfrequentie, hoe vaker de letter gemiddeld voorkomt in een tekst. De letterfrequentie is een handig hulpmiddel om substitutieversleutelingen mee te kraken. Als een letter veel voorkomt in de vercijferde tekst, is dit een letter die ook vaak voorkomt in de oorspronkelijke tekst. Als je weet welke letters vaak voorkomen (of juist weinig), kun je met de letterfrequentie bepalen naar welke letter ze waarschijnlijk vertaalt zijn in de vercijferde tekst.

Opdracht 6: Transpositieversleuteling

Vorm tweetallen. Jullie gaan elkaar een geheim bericht sturen.

(a) Verzin een geheim bericht en schrijf het op.

(b) Vercijfer het bericht als een transpositieversleuteling. Gebruik blokken van lengte 4. Stuur alle letters van positie 1 naar positie 3, van 2 naar 1, van 3 naar 4 en van 4 naar 2.

(c) Schrijf nu (samen) op hoe je een vercijferd bericht kunt ontcijferen, dus hoe je de letters moet verplaatsen om het bericht weer leesbaar te maken.

(d) Geef elkaar het vercijferde bericht en ontcijfer het. Klopt de ontcijfering met het originele bericht?

Opdracht 7: Caesarversleuteling

Hieronder staan caesarversleutelingen. Probeer de sleutel, dus hoe veel plaatsen elke letter verschoven is, te vinden. Je hoeft niet alle mogelijkheden uit te proberen, want je kunt gebruik maken van de Nederlandse letterfrequentie (zoek deze even op). Hierdoor komt de letter 'e' bijvoorbeeld vaak voor.

(a) ZUCEUJWUMEEDTUBUJJUHPYUDJULYDTUDTYUXUJCUUIJLEEHAECJ

(b) VJJAJUBMNJVNNAEXXATXVCMJWFXAMCQNCUJBCRP

Opdracht 8: Substitutie of transpositie?

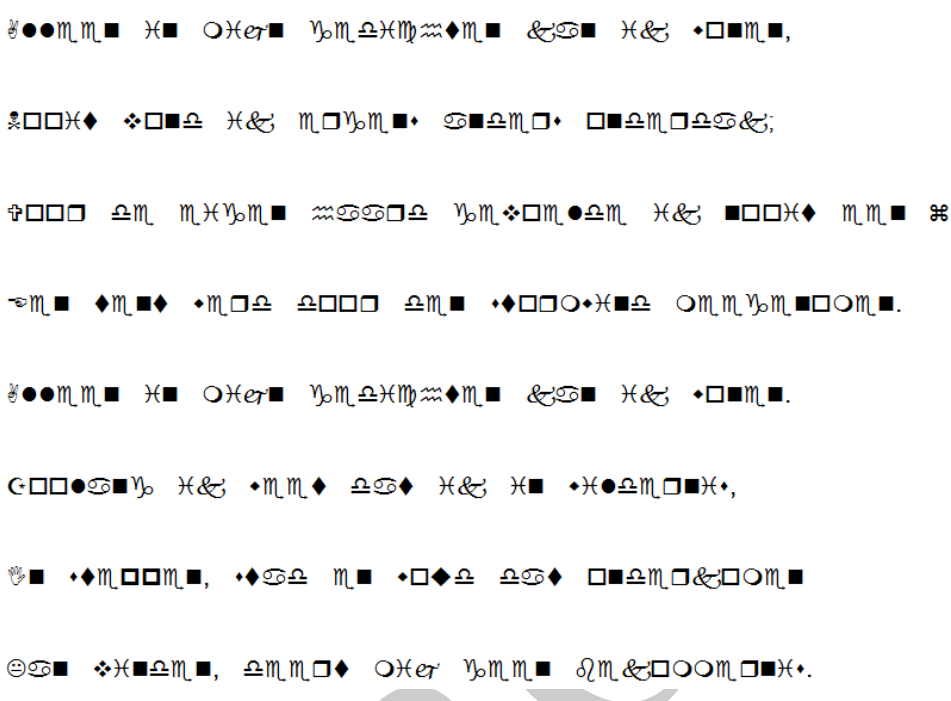
Bepaal met behulp van de letterfrequentie of het volgende bericht een substitutieversleuteling of een transpositieversleuteling is:
OIDZUBIRTEHEECTSSBNUITUTTEJIICEFOFROEHTCNARE
TSSONPTCEIIJREIFIANZJSDELJTNUIKLEZTEWTENEETEJH

Opdracht 9: Substitutieversleuteling

In Figuur 7 staat een substitutieversleuteling. Probeer het te ontcijferen door bij elk symbool de bijbehorende letter te vinden. De spaties, kommas en punten staan op de juiste plaats. Zoek de Nederlandse letterfrequentie op en maak hiervan gebruik om de eerste letters te vinden.

Opdracht 10: Veilig

Welke cijfer is moeilijker om te kraken, de caesarversleuteling of substitutieversleuteling? Beargumenteer je antwoord. Denk hierbij aan het aantal sleutels dat je kunt kiezen bij de cijfers. Waarom maakt het uit hoeveel het er zijn?



Figuur 7: Substitutieversleuteling

2.6 Moderne cijfers

Voorgaande cijfers waren allemaal niet erg veilig. Zeker met de hulp van een computer kun je het originele bericht achterhalen uit een vercijferd bericht zonder de sleutel te weten. De eerste standaard cryptografiemethode die op grote schaal werd gebruikt is **DES** (Data Encryption Standard).

DES is gebaseerd op een ontwerp van IBM, dat is aangepast door de NSA (National Security Agency) van de Verenigde Staten. De aanpassingen die de NSA gedaan had, maakten mensen achterdochtig. Ten eerste had de NSA de sleutellengte kleiner gemaakt dan in het ontwerp van IBM. Die kleinere sleutellengte zorgde ervoor dat het makkelijker werd om DES te kraken, maar het was nog steeds heel erg moeilijk. DES maakt gebruikt van S-boxen, die ingewikkelde combinaties van substitutie en transpositie toepassen op de tekst die vercijferd moet worden. In het begin werd niet bekend gemaakt hoe die S-boxen in elkaar zaten. Dit was een rede om te denken dat er een trucje in die S-boxen verwerkt was, waardoor de NSA met DES vercijferde tekst wel zou kunnen lezen. Zo'n trucje is nooit gevonden. Onderzoekers ontdekten na publicatie van de S-boxen zelfs dat de S-boxen goed tegen aanvallen bestand waren.

Doordat de computers sneller werden was het na een tijd mogelijk om DES te kraken. Een overheidsorganisatie van de Verenigde Staten, NIST (National Institute of Standards and Technology), organiseerde een wedstrijd om een betere standaard te vinden. Deze standaard kreeg de naam **AES** (Advanced Encryption Standard). Er werden vijftien methodes ingediend. Deze methodes werden beoordeeld aan de hand van een aantal criteria. Ten eerste moest de tijd waarin een tekst vercijferd en ontcijferd kon worden zo kort mogelijk zijn. Ten tweede moest de methode geschikt zijn voor de computeronderdelen (hardware) waarmee de vercijferd en ontcijferd werd. Ten derde moest het onmogelijk zijn om de methode te kraken. En zo waren er nog meer criteria. Uiteindelijk wonnen twee onderzoekers van de Katholieke Universiteit Leuven. Zij hadden een methode ontwikkeld die ze **Rijndael** noemden, naar hun namen Joan Daemen en Vincent Rijmen. AES wordt nu over de hele wereld gebruikt.

3 Asymmetrische cryptografie

3.1 Veel sleutels

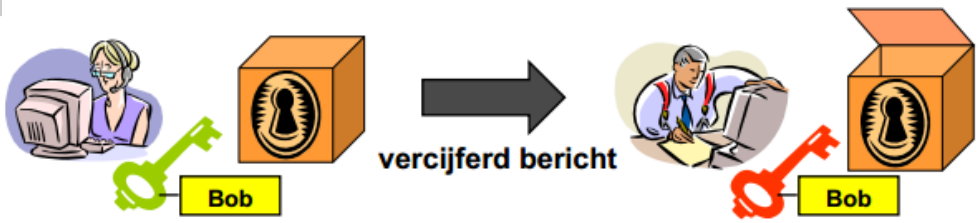
In het hoofdstuk 'Symmetrische cryptografie' heb je geleerd dat twee personen elkaar geheime berichten (dus onleesbaar voor anderen) kunnen sturen door een geheime sleutel te delen. Die geheime sleutel wordt dan gebruikt om de berichten onleesbaar en weer leesbaar te maken. Als je veel verschillende personen een geheim bericht wilt sturen, heb je voor ieder persoon een andere sleutel nodig. Je kunt je vast voorstellen dat je hierdoor heel veel sleutels nodig heb als iedereen met relatief veel personen wil communiceren. Bijvoorbeeld als je alle mensen op het internet veilig wil laten communiceren. Om precies te zijn, $\frac{1}{2}$n(n-1) sleutels voor n personen als iedereen met elkaar wil kunnen communiceren. Voor ieder persoon zijn er zijn namelijk n-1 andere personen als er n personen in totaal zijn. Dan zijn er n(n-1) sleutels nodig, alleen tel je dan iedere sleutel dubbel, omdat elke sleutel met z'n tweeën gedeeld wordt, dus moet je de helft van n(n-1) nemen. Omdat $\frac{1}{2}$n(n-1) = $\frac{1}{2}$n^2-n, dus het aantal sleutels kwadratisch is, neemt het aantal sleutels snel toe als n groter wordt. Dat terwijl je, zeker in de digitale wereld, veel contacten kunt hebben. Om een indruk te geven hoeveel sleutels dat wel niet zijn hieronder een tabel:

Aantal personen (n)	Aantal sleutels
2	1
10	45
100	4.950
1.000	499.500
10.000	49.995.000
100.000	4.999.950.000
1.000.000	499.999.500.000

3.2 Asymmetrische cryptografie

Asymmetrische cryptografie biedt een oplossing voor het grote aantal sleutels dat nodig is bij symmetrische cryptografie. Hierbij heeft ieder persoon een sleutel en een heel stel (hang)sloten die geopend kunnen worden met die ene sleutel. Als er niet genoeg sloten zijn, kunnen er gewoon bijgemaakt worden. De sleutel houdt je geheim, daarom wordt de sleutel vaak **privésleutel** genoemd. Het slot is openbaar, iedereen mag weten wat jouw slot is en het ook gebruiken. Het slot duiden we daarom ook wel aan met **publiek slot**.

Je vercijfert een bericht met het slot. Je kunt dit zien als het op slot doen (met het hangslot) van het bericht dat je wilt versturen. Je ontcijfert een bericht met de sleutel. Dit kun je zien als het openen van het hangslot met de sleutel, waardoor het bericht weer leesbaar wordt. Als Alice een bericht naar Bob wilt sturen gebruikt ze het slot van Bob om het bericht te vercijferen. Alleen Bob heeft namelijk de sleutel die bij dat slot hoort, dus hij is dan de enige die het bericht kan ontcijferen. Merk op dat zelfs Alice het bericht niet meer kan lezen zodra ze het vercijfert heeft met het slot.



Figuur 8: Asymmetrische cryptografie [groene sleutel moet hangslot worden]

3.3 Protocollen

In dit hoofdstuk zullen we niet ingaan op de cryptografische technieken die het mogelijk maken om digitale versies van dit soort sloten en sleutels te maken. Deze technieken liggen vooral op het gebied van de Wiskunde. We zullen wel ingaan op het juiste gebruik van deze sleutels en sloten. Het blijkt namelijk nog niet zo makkelijk te zijn om te voorkomen dat een kwaadwillende aanvaller (Eve) jouw geheime communicatie kan beïnvloeden. Om te kunnen achterhalen welke aanvallen mogelijk zijn schrijven we precies de stappen op die je zet om iets te communiceren. Net zoals bij een recept, alleen gaat het dan over de stappen die je moet zetten om iets te koken. De lijst met stappen die je zet om te communiceren noemen we een **protocol**.

Stel dat Alice wil inloggen op een webpagina. Ze stuurt dan haar gebruikersnaam en wachtwoord naar een server (een computer) die controleert of haar gebruikersnaam en wachtwoord juist zijn. Als ze kloppen stuurt de server de pagina waarop ze ingelogd is terug, anders stuurt de server dezelfde inlogpagina terug met de melding dat je gebruikersnaam en/of wachtwoord niet kloppen. Alice's wachtwoord en gebruikersnaam gaan over het internet naar de server, dus ze wilt niet dat iedereen ze kan lezen, dus kan ze ze beter vercijferd over het internet sturen. De vercijferde gebruikersnaam en wachtwoord zijn dan niet leesbaar, maar wel steeds hetzelfde als Alice telkens hetzelfde slot (van de server) gebruikt voor het vercijferen. Steeds een nieuw slot (en bijbehorende sleutel) maken is niet zo praktisch, doel was juist om niet zo veel verschillende sleutels en sloten nodig te hebben. Als de vercijferde gebruikersnaam en wachtwoord over het internet gaan kan Eve Alice's vercijferde gebruikersnaam en wachtwoord afluisteren. Later kan Eve ze dan opnieuw te sturen, waardoor het haar lukt om in te loggen als Alice.

Opdracht 11: Security doelen bij inloggen op webpagina

Er worden hierboven twee mogelijke aanvallen beschreven als Alice inlogt op een webpagina. Welke security doelen worden geschonden als Eve deze aanvallen kan uitvoeren?

3.4 Alice, Bob, Eve en Trent

In het hoofdstuk 'Inleiding cybersecurity' heb je al kennis gemaakt met Alice, Bob en Eve. Alice en Bob willen graag berichten naar elkaar sturen. Meestal stuurt Alice het eerste bericht. Eve probeert op alle mogelijke manieren Alice en Bob te dwarsbomen. Dit doet ze bijvoorbeeld door te proberen de (geheime) inhoud van berichten te achterhalen, berichten te veranderen of berichten te blokkeren. Hier introduceren we een nieuw personage: Trent. Hij helpt Alice en Bob bij het uitwisselen van hun berichten. Alice en Bob vertrouwen Trent volledig. Trent zal nooit geheime informatie, die hij van Alice of Bob krijgt, delen met anderen. Ook gaan Alice en Bob ervan uit dat alles wat ze van Trent krijgen klopt. Je zou Trent kunnen vergelijken met een notaris. Trent wordt ook wel 'Thrusted Third Party' genoemd.

3.5 Opdrachtinstructies

De volgende opdrachten gaan over protoollen en worden gedaan in groepjes. Ieder groepslid is een van de personages Alice, Bob, Eve en Trent. Als er te veel groepsleden zijn vervullen twee groepsleden de rol van een personage. Ieder personage heeft een aantal open hangsloten en een bijbehorende sleutel.

In sommige opdrachten speelt Trent geen rol. Dat groepsleden de rollen van verschillende personages op zich nemen betekent niet dat je niet onderling mag overleggen. Het uiteindelijke doel is om samen de opdrachten op te lossen.

Afsluitbare kistjes dienen als omhulsels voor berichten. Een bericht hoeft niet per se een stukje geschreven tekst op een blaadje te zijn, het mag bijvoorbeeld ook een hangslot zijn. Je kunt een bericht in het kistje stoppen en het daarna afsluiten met een hangslot door het hangslot dicht te klikken. Alleen degene met de bijbehorende sleutel kan dan het slot openmaken en het bericht lezen wat in het kistje zit. Zo kan iemand zonder de sleutel het bericht niet lezen. Je mag zoveel kistjes gebruiken als je wilt. Ook zien alle kistjes er hetzelfde uit. Dus kun je aan de buitenkant

niet zien welk bericht erin zit als je gezien zou hebben welke berichten in welke kistjes gingen. Het kistje met het bericht erin verstuur je door het kistje door te geven. Als een bericht niet geheim hoeft te blijven geef je het bericht gewoon door zonder kistje.

In de opdrachten ga je een aantal protocollen bekijken. Telkens sturen Alice en Bob (en soms Trent) berichten naar elkaar. Eve kan altijd zien wat er wordt gestuurd. Daarom moet een kistje van Alice, Bob of Trent altijd eerst aan Eve gegeven worden, waarna Eve het kistje weer doorgeeft.

Eve zou kunnen weigeren de kistjes door te geven, maar bij deze opdrachten is dat niet toegestaan (dat maakt de opdrachten wat saai). Ook zou Eve haar eigen slot op alle kistjes kunnen toevoegen, waarna ze het slot nooit meer verwijdert. Hierdoor kunnen de andere personages nooit een kistje openen. Gevolg is dat Alice, Bob en Trent niet meer kunnen communiceren. Dit is dan ook niet toegestaan bij deze opdrachten.

Ook zal Eve uiteindelijk minstens één bericht sturen aan de persoon waarvoor een bericht van Alice, Bob of Trent bedoeld was. Het is niet de bedoeling dat er iemand buitengesloten wordt. Kortom, Eve mag geen flauwe dingen doen waardoor Alice, Bob en/of Trent de kans niet krijgen om te communiceren.

Bij elke opdracht moet je precies noteren wat de stappen zijn die je doet. Een stap bestaat uit de actie die gedaan wordt, de voorwerpen die bij de actie gebruikt worden en het personage dat die actie uitvoert. Bij elk voorwerp moet duidelijk zijn van wie dat voorwerp is, behalve de kistjes, die zijn van iedereen.

Om duidelijk te maken wat precies de bedoeling is staat hieronder een opdracht met de oplossing erbij.

Opdracht 12: E-mail versturen

Opdracht: Alice wil een geheim bericht naar Bob sturen. Eve mag het bericht dus niet te lezen krijgen, maar de communicatie gaat wel via Eve. Schrijf hiervoor een protocol op. Speel het protocol na om te controleren dat het protocol ook echt klopt.
Beginsituatie: Alice en Bob hebben ieder hun eigen sleutel. Bovendien hebben Alice en Bob elkaars open hangsloten.

Antwoord:

1. Alice schrijft een geheim bericht.
2. Alice stopt haar bericht in een kistje.
3. Alice sluit het kistje met het slot van Bob.
4. Alice stuurt het kistje op weg naar Bob.
5. Eve ontvangt het kistje.
6. Eve stuurt het kistje naar Bob.
7. Bob ontvangt het kistje.
8. Bob opent met zijn sleutel zijn slot op het kistje.
9. Bob leest het geheime bericht.

Merk op: Bij stap 5 kan Eve het geheime bericht niet lezen.

3.6 Notatie

Je kunt je voorstellen dat dit al snel een lange lijst met stappen wordt als er meer berichten heen en weer gestuurd worden. Daarom introduceren we hier een notatie waardoor het korter en overzichtelijker wordt. Met A, B en E worden Alice, Bob respectievelijk Eve aangeduid. Met $\rightarrow$ geven we aan dat er een bericht verstuurd wordt, van het personage dat voor de pijl staat, naar

het personage dat na de pijl staat. Erachter zetten we een ':'. Daarachter schrijven we op wat de inhoud van het bericht is. Als Alice het bericht 'Hoi' verstuurd naar Bob, noteren we dit dus met:

$$A \to B : \text{Hoi}$$

Berichten kun je ook vercijferd versturen door ze in een kistje te doen en dicht te klikken met een slot, dus hier hebben we ook een notatie voor nodig. Stel dat Alice het bericht 'Hoi' in een kistje doet en het slot van Bob erop dichtklikt. Dan is de notatie:

$$A \to B : \{\text{Hoi}\}_B$$

Berichten in kistjes waarop geen slot zit zien we als berichten zonder kistje, dus dan gebruiken we de eerste notatie. De { en } staan voor het kistje, de $_B$ voor het hangslot waarmee het kistje is dichtgeklikt. Deze notatie en de hiervoor genoemde notatie zijn de standaard notatie in de security.

Soms willen we expliciet zeggen dat een personage een bericht kan lezen, al kun je dit meestal ook wel aflezen uit een vorige stap. Stel dat Bob het bericht 'Hoi' kan lezen (doordat hij eerder $\{Hoi\}_B$ heeft ontvangen), dan is de notatie als volgt:

$$B : \text{Hoi}$$

Behalve berichten kun je ook sloten in een kistje doen en die versturen. Als A haar (open) slot naar B stuurt gebruiken we de notatie:

$$A \to B : Slot_A$$

Met deze notatie wordt de oplossing van de opdracht 'E-mail versturen':

$$A \to E : \{\text{Geheim bericht}\}_B$$
$$E \to B : \{\text{Geheim bericht}\}_B$$
$$B : \text{Geheim bericht}$$

Opdracht 13: Uitgaan

In de opdracht 'E-mail versturen' hadden Alice en Bob van tevoren elkaars sloten al. Dat is natuurlijk niet altijd mogelijk. Wat kan Eve doen als Alice en Bob communiceren zonder de berichten te vercijferen? Schrijf onderstaand protocol eerst om naar de notatie. Bedenk vervolgens een aanval van Eve en verwerk Eve's acties in het protocol.

1. Alice stuurt het bericht 'Wil je met me uit, Bob? Liefs, Alice' (via Eve) op naar Bob.
2. Bob leest het bericht en stuurt 'Ja heel graag.' (via Eve) terug naar Alice.

Opdracht 14: Sloten uitwisselen

Je zag in de vorige opdracht dat Eve zonder gebruik van sloten de communicatie flink kon verstoren. Nu willen Alice en Bob de sloten uitwisselen door ze naar elkaar op te sturen, maar wel op een veilige manier. Alice, Bob en Eve hebben wel ieder hun eigen sloten en sleutels. Bekijk het volgende protocol:

1. Alice schrijft het bericht 'Mag ik jouw slot, Bob?' op.
2. Alice stuurt het bericht (via Eve) op naar Bob.
3. Bob stuurt (via Eve) een van zijn geopende hangsloten naar Alice.
4. Alice stopt het geheime bericht 'Wil je met me uit, Bob? Liefs, Alice' in een kistje.

5. Alice sluit het kistje met het slot dat ze ontving.

6. Alice stuurt het kistje (via Eve) naar Bob.

7. Bob opent het kistje met zijn sleutel.

8. Bob leest het bericht dat in het kistje zat.

Speel dit protocol na. Wat kan Eve doen doordat de berichten via haar gestuurd worden? Kan ze het geheime bericht van Alice te lezen krijgen? Of zelfs veranderen? Schrijf het protocol opnieuw op, met de dingen die Eve doet erbij. Doe dit met de geïntroduceerde notatie. Schrijf zo nodig eerst het oorspronkelijke protocol om naar de notatie.

Opdracht 15: Hulp van Trent

In de vorige opdracht zag je dat het mis ging met het verdelen van de sloten, niet iedereen kreeg het slot van de juiste persoon. De sloten van tevoren onder iedereen verdelen is veel gedoe. Maar het valt wel mee als ieder van te voren alleen bij Trent langs gaat, zijn of haar slot aan Trent geeft en Trent's slot mee terug neemt. De verdeling van de sloten is dan als volgt:

	Heeft sleutel van	Heeft slot van
Alice	Alice	Alice, Trent
Bob	Bob	Bob, Trent
Trent	Trent	Alice, Bob, Eve en Trent
Eve	Eve	Eve en Trent

(a) Bedenk een protocol waarin Alice, met de hulp van Trent, veilig een bericht aan Bob kan sturen. Gebruik dat Alice en Bob Trent volledig vertrouwen. Zorg dat Eve het bericht dat Alice naar Bob stuurt niet kan lezen.

(b) Bij de meest eenvoudige oplossing zal Eve nog wel extra berichten kunnen sturen aan Alice (of Bob) waarbij ze doet alsof Bob (of Alice) het bericht gestuurd heeft. Bij deze oplossing wordt niet vastgesteld wie een bericht heeft verstuurd heeft, dit leer je in het hoofdstuk. 'Identiteit en authenticatie' Hoe kan Eve deze extra berichten sturen en waarom?

Opdracht 16: Geheim voor Trent

Stel dat de sloten net zo verdeeld zijn als in de vorige opdracht. Maar nu willen Alice en Bob niet langer dat Trent hun berichten kan lezen. Is hiervoor ook een protocol te bedenken? Alice en Bob bedenken dat je behalve berichten ook sloten in een kistje kan doen en die opsturen. Hierdoor kan Alice aan Trent het slot van Bob vragen. Dit geeft het volgende protocol:

$$
\begin{aligned}
A \to T &: \text{Hoi Trent, mag ik het slot van Bob?} \\
T \to A &: \{Slot_B\}_A \\
A &: Slot_B \\
A \to B &: \{\text{Wil je met me uit, Bob? Liefs, Alice}\}_B \\
B &: \text{Wil je met me uit, Bob? Liefs, Alice}
\end{aligned}
$$

(a) Als je heel goed nadenkt, is deze oplossing niet juist! Eve kan de boodschap van Alice aan Bob onderscheppen. Waardoor komt dit? Schrijf met de notatie op hoe Eve de boodschappen kan lezen zonder dat Alice en Bob dit merken (dus het bericht komt gewoon aan bij Bob).

(b) Is er iets tegen deze aanval te doen? Verzin iets wat alleen Trent kan om duidelijk te maken dat een bericht echt van hem afkomstig is.

3.7 HTTPS

Als je naar een website waarvan de URL begint met 'https://' wordt er asymmetrische cryptografie gebruikt. De webpagina met alle gegevens die daar op staan wordt dan vercijferd (met asymmetrische cryptografie) over het internet naar jouw browser gestuurd. Hierdoor zijn bijvoorbeeld jouw bankgegevens afgeschermd als je gebruik maakt van internetbankieren. Je browser laat bij zo'n https-URL ook altijd linksboven in de URL-balk een gekleurd blokje zien met een hangslotje en het bedrijf waarvan de website is. Dat er een bedrijf genoemd wordt geeft aan dat je browser een digitaal bewijs van echtheid van de website heeft ontvangen. Zo'n bewijs wordt ook wel een **certificaat** genoemd.

3.8 Certificaten

Een certificaat bevat altijd de (digitale versie van) het publieke slot van een bedrijf en de datum waarop het certificaat verloopt. Na die datum geldt het certificaat niet meer, dus kun je er ook niet meer van uit gaan dat het vermelde slot van het bedrijf is. Een certicaat van Alice ziet er dus zo uit: "Het publieke slot van Alice is .... Dit certificaat is geldig van 23-05-2015 tot 23-09-2015."

De garantie dit cerificaat echt is, dus het het genoemde slot echt van Alice is, wordt gegeven doordat een bepaalde autoriteit zijn **digitale handtekening** op het certificaat zet. Zo'n autoriteit moet je dus vertrouwen om te kunnen concluderen dat het certificaat echt is. Als Trent het certificaat van Alice ondertekend zal Bob geloven dat het certificaat echt is, want Bob vertrouwd Trent. Dus na het controleren van Trent's handtekening weet Bob dus dat Trent gelooft dat het slot dat vermeld staat in het certificaat van Alice ook echt van Alice is. Trent gelooft dat omdat hij gecontroleerd heeft dat Alice het slot kan openen met haar sleutel en dat ze echt Alice is. Dat laatste kan Trent bijvoorbeeld controleren met de ID-kaart van Alice.

Opdracht 17: Bekijk certificaten in Firefox

Ongemerkt misschien gebruikt jouw browser een heleboel certificaten. In deze opdracht ga je certificaten bekijken in FireFox.

(a) Klik in FireFox bij 'Tools' op 'Options', daarna op het tabblad 'Advanced' en daarin op het tabblad 'Encryption'. Klik vervolgens op 'View Certificates'. Zoek bij de tabbladen 'Servers' en 'Authorities' naar bedrijven dat je kent en schrijf ze op.

(b) Bij 'Authorities' staan de certificaten die jouw browser vertrouwd. Bij 'Servers' de certificaten die door een van de 'Authorities' goedgekeurd zijn. Klik bij 'Severs' op een certificaat en dan op 'View'. Onder het kopje 'Issued To' staat over welke bedrijf dit certificaat gaat. Onder het kopje 'Issued by' staat welke 'Authority' dit certificaat heeft ondertekend. Onder 'Validity' staat vanaf welke tot welke datum het certificaat geldig is. Schrijf het bedrijf en de 'Authority' op. Noteer ook wanneer het certificaat geldig is. Controleer vervolgens of de gevonden 'Authority' ook te vinden is bij het tabblad 'Authorities'.

(c) Na het klikken op 'View' (in de Certificate Manager) kun je op het tabblad 'Details' klikken. Als je klikt op 'Subject's Public Key (even scrollen in 'Certificate Fields'). Krijg je onder 'Field Value' het (digitale) slot van dit certificaat te zien. N.B.: je ziet hier de cijfers 0 t/m 9 en a t/m f, omdat hier hexadecimale notatie is gebruikt i.p.v. decimale notatie. Wat is het digitale slot van het certificaat dat je bekeken hebt bij (b)?

(d) Welke https-website ken je? Ga naar een zo'n https-website en klik op het slotje in de URL-balk. Klik vervolgens op 'View Certificate'. Nu krijg je het certificaat te zien dat bij deze website hoort, net zoals bij (b). Noteer voor dit certificaat de gegevens die in (b) gevraagd werden.

3.9 Extra: digitale handtekening

Bij het zetten van een digitale handtekening worden ook een sleutel en bijbehorend slot gebruikt, alleen net andersom als bij het vercijferen van een bericht. In het geval dat Trent zijn handtekening zet op het certificaat van Alice, 'plakt' Trent eerst zijn sleutel vast aan het certificaat van Alice. Vervolgens kan iedereen, dus ook Bob, een publiek slot van Trent nemen en met die vastgeplakte sleutel controleren dat het slot open gaat. Hierdoor weet je dat het slot bij de sleutel hoort, anders had je het slot niet open kunnen maken. Bob vertrouwt Trent, dus hij gelooft het dat als Trent hem zijn slot geeft dat slot ook daadwerkelijk van Trent is. De 'vastgeplakte' sleutel op het certificaat kun je alleen gebruiken om een los slot te openen, en niet om een slot op een bericht te openen. Eigenlijk dient het slot nu als een sleutel en de sleutel als een slot. In de security worden het slot en de sleutel daarom allebei sleutel genoemd: **private key** voor de sleutel en **public key** voor het slot.

4 Authenticatie

4.1 Identiteit vs Authenticatie

In het hoofdstuk 'Inleiding cybersecurity hebben we het al even over **authenticatie** gehad. Als je je authenticeert dan bewijs je wie je bent. Bijvoorbeeld met je ID of paspoort bij de douane (gezichtsherkenning), je wachtwoord op Facebook, je PIN-code bij de pinautomaat of met stemherkenning als je een bekende aan de telefoon hebt. Bewijzen wie je bent is niet hetzelfde als zeggen wie je bent. Voorbeelden van zeggen wie je bent zijn je naam, je loginnaam, je bankrekeningnummer en je BSN (BurgerServiceNummer). Als je alleen zegt wie je bent noemen we dat **identificatie**. Als iemand om jouw naam vraagt, zeg je meestal je eigen naam. Maar er is geen bewijs. Een nieuwe leraar kun je best (even) voor de gek houden door een andere naam te noemen.

Opdracht 18: identificatie of authenticatie?

Geef van onderstaande gevallen aan of het hier om identificatie of authenticatie gaat.

(a) De nummerplaat van een auto.

(b) Je schoolpas.

4.2 Autorisatie

Als je inlogt op een webpagina heb je vaak de beschikking over bepaalde acties die je mag uitvoeren. Je mag bijvoorbeeld een berichtje posten op een forum. Dat berichtje mag je vaak ook nog aanpassen. Andere mensen mogen echter niet jouw bericht aanpassen. Je mag alleen je eigen berichten aanpassen. Vaak zijn er wel moderators die zorgen dat iedereen zich aan de regels houdt. Die mogen wel jouw berichten aanpassen. We zeggen ook wel dat de moderator de **autorisatie** heeft om jouw berichten aan te passen. Voor de acties die je mag doen maakt het dus uit of je moderator bent of een gewone gebruiker.

De autorisatie, dus de acties die jij mag doen, wordt bepaald aan de hand van je identiteit. Die identiteit is bewezen met authenticatie doordat je hebt inlogt met je wachtwoord. De webpagina zal eerst controleren of je toegang hebt (authenticatie) en daarna welke acties je mag doen (autorisatie) doordat bij het inloggen is vastgesteld of jij een moderator of een gewone gebruiker bent.

4.3 Authenticatie aan een computer

Het is vaak makkelijk en snel om via internet geld over te maken, aankopen te doen, je in te schrijven voor en studie of belastingaangifte te doen. Bij al dit soort dingen is het belangrijk dat je bewijst wie je bent, want niet iedereen mag deze acties uitvoeren. Het is bijvoorbeeld niet de bedoeling dat iemand zomaar geld van jouw internetbankieraccount overmaakt naar zijn eigen rekening. Jij moet je dus authenticeren aan de website (of een ander programma). Die website wordt door een server (een computer) naar jouw computer gestuurd. Die server wil dus vaststellen wie jij bent.

In het algemeen zijn er drie manieren waarmee een mens zich aan een computer kan authenticeren:

- Met **iets wat je hebt**, dus een voorwerp. Bijvoorbeeld een autosleutel of een bankpas.
- Met **iets wat je bent**, dus een kenmerk wat uniek is voor jou. Bijvoorbeeld je vingerafdruk of je foto.
- Met **iets wat je weet**, dus een wachtwoord. Bijvoorbeeld een (standaard) wachtwoord van enkele letters, cijfers en/of vreemde tekens lang, een PIN-code, of het antwoord op een vraag.

Iets wat je hebt moet je eerst (in de fysieke wereld) ophalen. Bij een auto is dit natuurlijk geen probleem, want je wilt de auto ook hebben. Maar voor een bankpas of een andere smart-card is het minder wenselijk. Per post toezenden is soms ook een optie, al moet je dan wel zeker zijn dat het bij de juiste persoon aankomt. Anders kan degene die het voorwerp onderschept zich zomaar (ten onrechte) authenticeren! Andere nadelen zijn dat het voorwerp gestolen of nagemaakt kan worden.

Iets wat je bent moet je vaak op een één of andere manier vastleggen om mogelijk te maken dat iemand anders daarmee kan controleren of jij het bent. Er moet eerst een foto gemaakt worden om de foto te kunnen vergelijken met je gezicht. Je vingerafdruk laat je scannen of zet je op papier met inkt. Vaak kun je iets wat je bent niet veranderen. Als je vingerdruk op internet is gezet kan iedereen die dat wil een nepvinger maken met die vingerafdruk. Met die nepvinger kan iemand zich dus als jou authenticeren. Alles plekken waar jij je authenticeert met je vingerafdruk moeten dan geblokkeerd worden, om te voorkomen dat je de dupe wordt van de kapotte beveiliging. Je vingerafdruk kun je de rest van je leven dan niet meer gebruiken voor authenticatie.

Om een wachtwoord op te geven hoef je niets te doen in de fysieke wereld. Je gaat gewoon even naar een webpagina waar je je wachtwoord opgeeft. Het gemak van wachtwoorden is de reden dat ze zoveel gebruikt worden. Maar ook wachtwoorden hebben nadelen. Iemand kan meekijken als je je wachtwoord intypt en wachtwoorden kun je vergeten. Een actieve aanvaller zal ook alle mogelijke wachtwoorden uitproberen (brute force aanval), als dat mogelijk is. Of je opbellen en zich voordoen als iemand die het systeem onderhoudt of iets dergelijks, waarvoor hij jouw wachtwoord nodig hebt. Dit laatste is een voorbeeld van **social engineering**. Bij social engineering probeert de aanvaller om iets van jou te achterhalen door zich voor te doen als iemand die jij (in eerste instantie) vertrouwt en het dan gewoon te vragen. Er is ook een heleboel malware (kwaadaardige software) die als doel heeft om jouw wachtwoorden te achterhalen. Meer hierover volgt in het hoofdstuk 'Digitale gevaren'.

Opdracht 19: Iets wat je hebt, bent of weet?

Hieronder staan voorbeelden van manieren om te authenticeren. Bepaal of dit authenticatie is met iets wat je hebt, iets wat je bent of iets wat je weet. Als er meerdere mogelijkheden zijn, kies dan wat het beste past.

(a) Het laten zien van een identiteitskaart.

(b) Een stempel op je arm die aangeeft dat je toegang hebt betaald voor een bepaalde feestgelegenheid.

(c) Een handtekening zetten.

(d) Swipe-authenticatie op je smartphone.

4.4 Veilige wachtwoorden

De meeste wachtwoorden die mensen kiezen zullen niet bestand zijn tegen een brute force attack (waarbij de aanvaller de beschikking heeft over zoveel computers als nodig). Een wachtwoord is pas echt veilig als hij bestaat uit:

- 11 willekeurig (door de computer) gekozen tekens
- 16 door de computer gekozen tekens die samen een woord vormen dat je kunt uitspreken
- 32 door jou gekozen tekens

Een trucje om een lang wachtwoord te onthouden is om een zin te gebruiken, waarbij je de woorden aan elkaar plakt. Die zin moet natuurlijk niet heel makkelijk te raden zijn, maar voor jou wel makkelijk te onthouden zijn. Zo'n zin wordt **pass phrase** genoemd. Je kunt ook die zin

weer afkorten om een korter wachtwoord te krijgen. De zin 'Ik heb drie honden en die lusten kilo's Bonzo-koekjes.' wordt bijvoorbeeld 'Ih3h&dlk'sB'.

Nadeel van lange wachtwoorden is dat je snel een typefout maakt. Ook is het misschien niet nodig dat je wachtwoord tegen de allersterkste aanval kan, omdat de informatie of dienst die het wachtwoord beschermd niet erg belangrijk is. Bijvoorbeeld als je een eenmalige aankoop doet bij een webwinkel en je daarvoor een account moet aanmaken. Je naam en adres moet je dan invullen, maar andere gegevens heeft de webshop niet nodig. Als je toch verplicht wordt om onnodige gegevens in te vullen, kun je iets verzinnen. Meestal wordt ook om een e-mailadres gevraagd. Voor dit soort zaken kun je een apart e-mailadres aanmaken, zodat de webshop niet achter de e-mailadressen komt die je dagelijks gebruikt.

4.5 Richtlijnen

Hieronder staan een aantal richtlijnen[1] die je helpen om goed om te gaan met wachtwoorden:

1. Kies op internet voor elke website een ander wachtwoord. In ieder geval voor belangrijke websites. Je loginnaam is meestal bekend, want dat is vaak ook de naam die andere gebruikers kunnen zien. Als je een wachtwoord op verschillende websites gebruikt, kan een aanvaller met die loginnamen gelijk op al die websites inloggen.
2. Vertel wachtwoorden aan niemand. Ook al vertrouw je iemand volledig. Mocht dit in de toekomst veranderen of niet terecht zijn, dan heb je daar geen last van.
3. Verander wachtwoorden die je toegewezen krijgt. De persoon of instantie die jou dit wachtwoord heeft toegewezen is namelijk ook op de hoogte van dit wachtwoord.
4. Verander je wachtwoord als je hem per ongeluk verklapt hebt.
5. Kies degelijke wachtwoorden. Kies moeilijkere wachtwoorden voor dingen die belangrijk zijn. Zorg dat wachtwoorden niet makkelijk te raden zijn, minimaal 8 tekens lang en gebruik het hele toetsenbord om je wachtwoord samen te stellen.
6. Je wachtwoord op papier opschrijven is acceptabel als je het thuis bewaart.
7. Bewaar je wachtwoorden nooit op een documentje op je computer of mobiel.

Opdracht 20: Gebruik jij veilige wachtwoorden?

(a) Ga na aan welke richtlijnen je voldoet. Hoeveel zijn het er?

(b) Zitten er richtlijnen tussen waar je nog nooit aan gedacht had? Welke zijn dat?

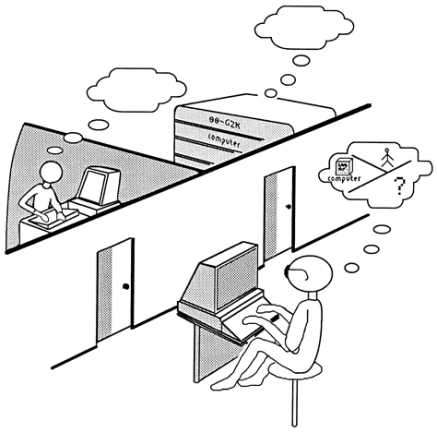
4.6 Turingtest

Soms wil je alleen vaststellen dat iemand een mens is. Vaak om te voorkomen dat programmaatjes (meestal 'bots' genoemd) bepaalde acties uitvoeren i.p.v. een mens. Hiervoor worden vaak **captcha** (completely automated public Turingtest to tell computers and humans apart) gebruikt. Je moet dan de tekens die (vervormd) zijn afgebeeld overtypen. Je ziet captcha's vaak op fora. Ook moet je een captcha invullen als je een Gmailaccount aanmaakt.

Een captcha is een specifieke vorm van een **Turingtest**. Bij een Turingtest wordt alleen door (digitaal) te communiceren bepaald of er met een mens of een computer gecommuniceerd wordt. Deze test is bedacht door Alan Turing, voordat computers bestonden! Behalve van de Turingtest is Turing ook bekend van het kraken van de Enigma-machine, een apparaat waarmee de Duitsers in de Tweede Wereldoorlog berichten mee vercijferden en ontcijferden.

[1] Copyright leowillems.nl

Figuur 9: Captcha
http://depletedcranium.com/stopping-spam-and-deciphering-text-too/



Figuur 10: Turing test
http://www.alanturing.net/turing_archive/pages/reference%20articles/theturingtest.html

4.7 Gebruik van cryptografie voor authenticatie

Je wilt niet dat andere mensen erachter kunnen komen wat jouw wachtwoord is. De bolletjes die verschijnen als je je wachtwoord typt zorgen ervoor dat iemand niet op je scherm kan lezen wat je wachtwoord is. Maar je wilt ook niet dat je wachtwoord bekeken wordt als je op 'Login' drukt en hij dus over internet verstuurd wordt. Cryptografie kan hierbij helpen. Als je een wachtwoord vercijferd is hij namelijk niet meer leesbaar. De ontvanger kan het bericht dan ontcijferen en het wachtwoord controleren. Je moet echter wel heel erg opletten hoe je dit doet, dus welk protocol je gebruikt. Soms kan een aanvaller de boel toch nog verstoren. In de volgende opdrachten zal dit duidelijk gemaakt worden.

Opdracht 21: Autosleutels

We willen op een veilige manier een auto open maken met een (elektronische) autosleutel. Hieronder worden een aantal mogelijkheden gegeven. Beantwoord voor elk van die mogelijkheden de volgende vragen:

(i) Is dit veilig?

(ii) Zo ja, waarom? Zo nee, welke aanval is er mogelijk en zou je deze kunnen voorkomen?

Er zal gebruik gemaakt worden van symmetrische cryptografie. We zullen een aangepaste notatie gebruiken zoals die in het hoofdstuk 'Asymmetrische cryptografie' is uitgelegd (kijk even terug als je die niet meer weet). De letter 'A' staat voor de auto en de letter 'AS' voor de autosleutel. De auto en de autosleutel delen de (cryptografische) sleutel 'K' (van 'key'). We noteren een versleuteld

bericht als K{bericht}. Dit is dus een andere notatie om een bericht te versleutelen. Door deze andere notatie is duidelijk dat het hier om symmetrische cryptografie gaat i.p.v. asymmetrische cryptografie. We nemen Eve weer als de aanvaller en noteren haar met 'E'. Alle berichten gaan via haar.

(a) Hieronder geven we met 'IdNr' een nummer aan dat uniek is per auto. De auto controleert in de laatste stap het IdNr controleren en de auto openen.

$$\begin{aligned} AS \rightarrow A &: IdNr \\ A &: IdNr \end{aligned}$$

(b) Nu versleutelen we het IdNr:

$$AS \rightarrow A : K\{IdNr\}$$

(c) Met 'N' geven het nummer aan van een tellertje dat de auto en de autosleutel bijhouden. Elke keer als de auto geopend wordt, wordt het tellertje in de auto met één opgehoogd. Elke keer als je de autosleutel gebruikt, wordt het tellertje in de sleutel met één opgehoogd. Bij de laatste stap controleert de auto dat N de waarde is van het tellertje en gaat de auto open. Door een tellertje te gebruiken, wordt er nooit hetzelfde nummer gebruikt. Hierdoor is de versleuteling van dat tellertje telkens anders. Als je N en N+1 versleutelt kun je aan die versleutelingen niet zien welke de grootste en welke de kleinste is.

$$\begin{aligned} AS \rightarrow A &: K\{N+1\} \\ A &: N+1 \end{aligned}$$

(d) Nu houdt alleen de auto het tellertje 'N' bij. De autosleutel hoeft niks te onthouden. Bij de laatste stap controleert de auto dat N de waarde is van het tellertje en gaat de auto open.

$$\begin{aligned} AS \rightarrow A &: \text{Open} \\ A \rightarrow AS &: K\{N\} \\ AS &: N \\ AS \rightarrow A &: K\{N+1\} \\ A &: N+1 \end{aligned}$$

Opdracht 22: Wachtwoord

(a) Bedenk een aanval op het volgende protocol. Er wordt gebruik gemaakt van asymmetrische cryptografie. Alice wil zeker weten dat ze met Bob communiceert en vraagt daarom om het wachtwoord dat ze van tevoren hebben afgesproken. Alice en Bob hebben dit wachtwoord nog nooit gebruikt en gebruiken het ook maar één keer. Bob en Eve hebben beiden het publieke slot van Alice.

$$\begin{aligned} A \rightarrow B &: \text{Wat is het geheime wachtwoord? Groetjes Alice} \\ B \rightarrow A &: \{\text{Het geheime wachtwoord}\}_A \end{aligned}$$

(b) Verbeter het bovenstaande protocol. Maak gebruik van het feit dat je meerdere sloten op een kistje kunt bevestigen. Noteer een bericht waaraan de sloten van Alice en Bob bevestigt zijn met $\{\text{Bericht}\}_{A,B}$. Bob en Alice hebben elkaars publieke sloten niet nodig.

5 Digitale gevaren

5.1 Spam

Met z'n allen versturen we veel e-mail, meer dan 2 miljoen e-mailtjes per seconde! E-mail is dan ook erg handig, een e-mailtje komt bijna gelijk bij de ontvanger aan, mag zo lang zijn als je wilt, is (meestal) gratis en je kunt ook nog allerlei bestanden als bijlage meesturen. Deze eigenschappen van e-mail kunnen echter ook misbruikt worden.

Veel van de e-mails die verstuurd worden vallen onder **spam**: ongewenste berichten die massaal verspreid worden. Zo'n 80 tot 98 procent van de e-mails is spam. Gelukkig bestaan er ook spamfilters, waardoor je niet alle spam in je inbox krijgt. Toch glipt er nog wel eens een spam-mailtje doorheen.

Veel spam-mailtjes bevatten reclame advertenties. Er zijn misschien weinig mensen die ook daadwerkelijk iets kopen door een advertentie. Daar tegenover staat dat de advertenties per mail naar vele miljoenen mensen verstuurd kunnen worden. Dus ook als maar een klein percentage mensen iets van de advertenties koopt, zijn dit er relatief veel mensen doordat zoveel mensen een mailtje binnenkrijgen. Behalve advertenties kan een spam-mailtje ook andere dingen bevatten, zie de volgende paragraaf.

Hierdoor is spammen best aantrekkelijk. Om te kunnen spammen zijn wel een aantal dingen nodig die vaak wat kosten. De overige winst is voor de spammer. De producten die de advertentie verkoopt, moeten gemaakt worden. Bovendien wil de verkoper (als dit niet de spammer is) er ook winst op maken. Verder moet er een website zijn waarop de producten verkocht worden. Ook moeten e-mail adressen verzameld worden. Vervolgens moet er een netwerk van computers ingezet worden om al die e-mails te kunnen verzenden en onzichtbaar te maken waar de spam vandaan komt. Dit heet een **botnet**. Zo'n botnet bestaat vaak uit computers van andere (onwetende) mensen, die een keer besmet zijn door malware (kwaadaardige software). Over malware volgt later informatie.[2]

Opdracht 23: Heb jij spam in je inbox?

(a) Hoeveel e-mailtjes met een onbekende afzender heb je afgelopen maand ontvangen? Vergeet niet in je Spam-folder en/of verwijderde mailtjes te kijken.

(b) Hoeveel mailtjes met reclame heb je afgelopen maand ontvangen?

(c) Hoeveel ongewenste berichten heb je afgelopen maand ontvangen? Vergelijk dit aantal met het aantal e-mails dat wel van belang was voor jou. Welk percentage van al je ontvangen e-mails is spam?

5.2 Phishing

Bij **phishing** doen criminelen zich voor als een vertrouwde persoon of instantie om zo gevoelige informatie te verkrijgen, bijvoorbeeld inloggegevens van internetbankieren. Die gegevens worden verkregen door het slachtoffer bijvoorbeeld naar een vervalste website te leiden of te zorgen dat er malware wordt geïnstalleerd op de computer van het slachtoffer. Het slachtoffer daartoe verleidt via communicatiemiddel. Vaak is dit een e-mailtje. Zo'n e-mail valt dan onder spam. Soms wordt een slachtoffer opgebeld. De crimineel doet zich dan bijvoorbeeld voor als ICT-medewerker, zoals in opdracht 1.7(b).

Zoals bij spam al is opgemerkt, kan een e-mailtje gemakkelijk naar vele e-mailadressen gestuurd worden, waardoor veel mensen bereikt worden. Hoe meer mensen, hoe groter de kans dat iemand het phishing-mailtje gelooft. Behalve voor advertenties is e-mailen dus ook aantrekkelijk voor phishing.

[2]Gebaseerd op notes van Leo Willems (Copyright leowillems.nl)

Vaak zijn er aanwijzingen dat een e-mail een phishing-mail is. Verder helpt het om kritisch na te denken. Als je een phishing-mail herkent, kun je voorkomen dat je slachtoffer wordt. Hieronder een aantal richtlijnen[3] om phishing te voorkomen:

1. De afzender kan wel eens iemand anders zijn dan dat er staat. Vertrouw nooit blindelings op de afzendergegevens. E-mails van onbekende afzenders kun je beter niet openen.
2. Ga na of de inhoud van het bericht wel past bij de organisatie of de persoon die het bericht stuurt. Als dit niet klopt, dan is het mogelijk een phishing-mail.
3. Reageer niet op waarschuwingen voor virussen of andere gevaren. Dit zijn in werkelijkheid kettingbrieven.
4. Klik nooit op onbekende links, zeker niet als de link er raar uit ziet. Wil je de link toch bezoeken, type dan zelf de link in je browser. Als je erop klikt of de link kopieert, kan je namelijk alsnog naar een andere website gestuurd worden dan er staat.
5. Download geen onbekende bijlagen van e-mail berichten die je niet vertrouwd. Als je dit wel doet kun je malware op je computer geïnstalleerd krijgen.
6. Grammatica- en spelfouten zijn een aanwijzing dat de e-mail een phishing-mail is. Negeer deze e-mails.
7. Geef nooit financiële gegevens of privé gegevens af. Er zal door de bank zelf nooit om inloggevens voor internetbankieren en dergelijke dingen gevraagd worden.
8. Let op de veiligheid van het medium als je gevoelige gegevens als burgerservicenummers, bankrekeningnummer en privé gegevens van vrienden uitwisseld. Vermijdt voor het uitwisselen van dit soort gegevens, als het even kan, cloud applicaties, mobiele applicaties en e-mail berichten.
9. Denk je dat je slachtoffer geworden bent? Wijzig dan zo mogelijk je gegevens, bijvoorbeeld je wachtwoord als je die hebt afgegeven.

Opdracht 24: Gevoelig voor phishing?

(a) Heb je wel eens een van bovenstaande richtlijnen geschonden? Welke richtlijnen waren dat?

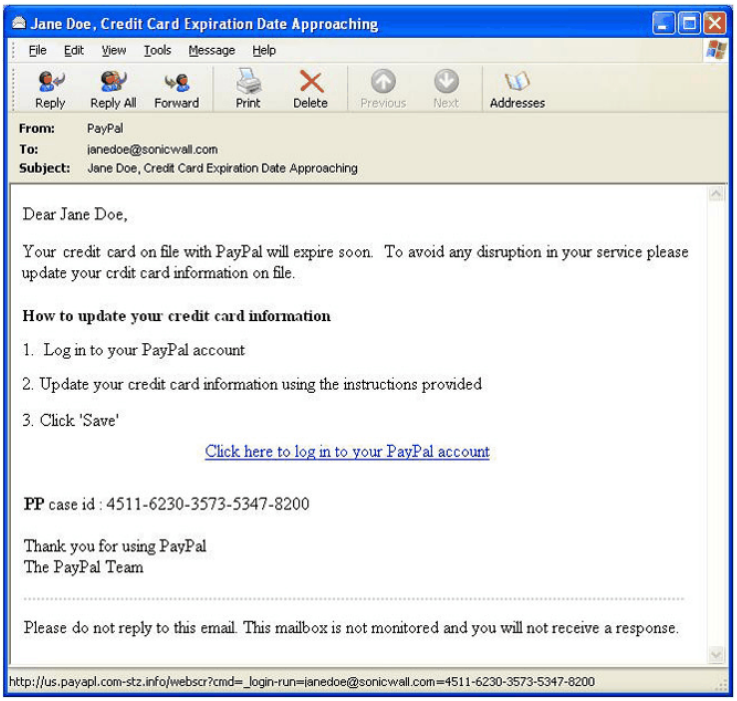
(b) Zo ja, wat waren de gevolgen?

Opdracht 25: Phishing-mails herkennen

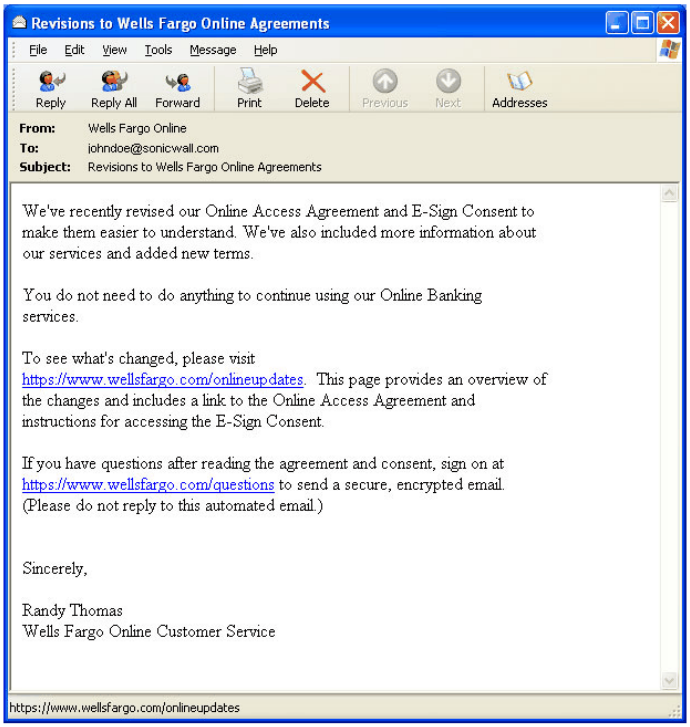
Bepaal voor elk van de volgende voorbeelden[2] of er sprake is van phishing. Beschrijf welke aanwijzingen jouw standpunt ondersteunen.

[3]Gebaseerd op notes van Harald Vranken

(a)


Jane Doe, Credit Card Expiration Date Approaching
File Edit View Tools Message Help
Reply Reply All Forward Print Delete Previous Next Addresses
From: PayPal
To: janedoe@sonicwall.com
Subject: Jane Doe, Credit Card Expiration Date Approaching
Dear Jane Doe,
Your credit card on file with PayPal will expire soon. To avoid any disruption in your service please update your crdit card information on file.
How to update your credit card information
1. Log in to your PayPal account
2. Update your credit card information using the instructions provided
3. Click 'Save'
Click here to log in to your PayPal account
PP case id : 4511-6230-3573-5347-8200
Thank you for using PayPal
The PayPal Team
Please do not reply to this email. This mailbox is not monitored and you will not receive a response.
http://us.payapl.com-stz.info/webscr?cmd=_login-run=janedoe@sonicwall.com=4511-6230-3573-5347-8200

(b)


Revisions to Wells Fargo Online Agreements
File Edit View Tools Message Help
Reply Reply All Forward Print Delete Previous Next Addresses
From: Wells Fargo Online
To: johndoe@sonicwall.com
Subject: Revisions to Wells Fargo Online Agreements
We've recently revised our Online Access Agreement and E-Sign Consent to make them easier to understand. We've also included more information about our services and added new terms.
You do not need to do anything to continue using our Online Banking services.
To see what's changed, please visit https://www.wellsfargo.com/onlineupdates. This page provides an overview of the changes and includes a link to the Online Access Agreement and instructions for accessing the E-Sign Consent.
If you have questions after reading the agreement and consent, sign on at https://www.wellsfargo.com/questions to send a secure, encrypted email. (Please do not reply to this automated email.)
Sincerely,
Randy Thomas
Wells Fargo Online Customer Service
https://www.wellsfargo.com/onlineupdates

(c)

Rabobank

Customer Services Update

Om ervoor te zorgen uw bescherming, hebben we nu uitgeschakeld toegang tot uw rekeningen. U moet nu opnieuw instellen uw veiligheid. U zult niet in staat zijn om toegang tot uw rekeningen te krijgen totdat je dit hebt gedaan.

Informatie - Als u uw toegangscode niet binnengaan van uw willekeurige kaartlezer of uw Rabo-kaart te verwijderen uit de Random Reader apparaat na verificatie vriendelijk geduldig te zijn voor 15 tot 20 minuten kunnen we dan controleren of uw gegevens kunt u uw rekening.

Onze excuses voor het ongemak

Om te beginnen de reactivering proces, gelieve de verwijzing onderstaande link te zien.
klikken hier.

Afdeling internetbankieren

F Brazier

E-Communicatie-eenheid
Rabobank.

(d)

Beste Klant,

Zoals u reeds heeft vernomen hebben wij als SNS Bank. enige tijd geleden te maken gehad met een fusie van de huidige SNS Bank met het voormalige Postbank.
Voor de klant is er overigens weinig veranderd, echter achter de schermen hebben wij een totaal nieuwe internetapplicatie geprogrammeerd die aan de hedendaagse veiligheidseisen voldoet comform de Europese richtlijnen betreft het betalingsverkeer.
Bij een verbetering (update) van ons online veiligheidssysteem hebben wij bij uw rekening een foutmelding ontvangen met als code ASV-317.
Deze foutmelding is simpel te verwerken door de upgradepagina te downloaden die u kunt vinden als bijlage in deze mail.
Vul het formulier in en login op uw account.
Zodra u heeft ingelogd kunnen wij het proces afronden en krijgt u binnen 7 werkdagen een geautomatiseerde bevestigingsmail toegestuurd.

5.3 Scareware

De bedoeling van **scareware** is om de computergebruiker bang te maken, waardoor hij eerder geneigd is een boete te betalen, gegevens af te staan of (kwaadaardige) software te installeren of een combinatie daarvan. Scareware kan als malware binnenkomen, of als popup op een website getoond worden. In Figuur 11 staan twee voorbeelden van scrareware.

http://lastwatchdog.com/scareware-promotions-spreading-google-youtube/

http://www.pchulplijn.nl/buma_stemra_virus_verwijderen

Figuur 11: Scareware

5.4 DDoS aanval

De afkorting **DDoS** staat voor Distributed Denial of Service. DDoS aanvallen zorgen ervoor dat het systeem wat aangevallen wordt onbeschikbaar is, dus niet gebruikt kan worden door de bedoelde gebruikers. Vaak is het systeem dat wordt aangevallen een belangrijke website, bijvoorbeeld de website van een bank waar je kunt internetbankieren. Een DDoS aanval kan worden uitgevoerd door bijvoorbeeld malware te installeren op het systeem, of door met een botnet zoveel verbindingen op te zetten dat er geen nieuwe verbindingen gemaakt kunnen worden. Een enkele keer wordt er onbedoeld een DDoS aanval uitgevoerd op een website, bijvoorbeeld als heel veel mensen een concertkaartje willen kopen.

Opdracht 26: Recentste DDoS aanval

(a) Wanneer was de recentste DDoS aanval?

(b) Welk systeem werd er aangevallen?

(c) Wat was de rede of zou een mogelijke rede kunnen zijn?

(d) Hoe is ervoor gezorgd dat de aanval stopte? Is er iets gedaan om DDoS-aanvallen in het vervolg te voorkomen?

5.5 Malware

Malware staat voor 'malicious software' ofwel kwaadaardige software. Het doel van malware is dus om iets kwaadaardigs te doen op of met je computer, bijvoorbeeld spam verzenden als onderdeel van een botnet, wachtwoorden verzamelen, privacy gevoelige gegevens verzamelen enz. We zullen hier de drie belangrijkste vormen van malware bespreken: wormen, virussen en trojan horses.

5.5.1 Worm

Een (computer)**worm** is een computerprogramma dat zichzelf, zonder hulp van een mens, kan verspreiden, meestal over een computernetwerk. Een **computernetwerk** verbindt computers aan elkaar zodat de computers data uit kunnen wisselen. Het meest bekende computer netwerk is het internet. Een ander voorbeeld van een computer netwerk is dat computers van een bedrijf of school met elkaar verbonden zijn, waardoor data gemakkelijk kan worden uitgewisseld. Bij scholen kan een leerling vaak inloggen op elke computer. Een worm kan zich verspreiden over een computer netwerk door zichzelf te kopiëren en gebruik te maken van fouten die zijn gemaakt bij het beveiligen van het computernetwerk. Meestal zijn dit fouten in de besturingssystemen (bijv. Windows, MacOSX of Linux) die draaien op de computers van het netwerk.

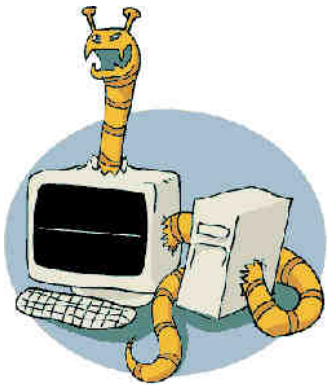
Doordat een worm zichzelf kopieert en verspreid over het netwerk richt hij al schade aan, doordat er nu vooral wormen over het netwerk gaan in plaats van de data die er normaal gesproken overheen ging. Een computernetwerk kan namelijk maar een bepaalde hoeveelheid dataverkeer aan. De eerste worm, de Morris Worm, was een worm die zichzelf alleen verspreidde. Maar er zijn ook wormen die meer doen dan alleen verspreiden. Wormen kunnen namelijk een programmaatje met zich meenemen. Zo'n programmaatje verwijdert bijvoorbeeld bestanden op de computer waar de worm is aangekomen, vercijfert bestanden (waardoor je ze niet meer kan lezen) of installeert programma zodat de computer onderdeel wordt van een botnet.

Opdracht 27: ILOVEYOU worm

Zoek de volgende dingen op over de ILOVEYOU worm:

(a) Wat deed de worm?

(b) Hoe verspreidde de worm zich?



Figuur 12: Computerworm
http://www.lantech.co.nz/?sn=66&st=1&pg=1962

(c) Waarom was deze worm zo effectief?

5.5.2 Virus

Een (computer)**virus** is een computerprogramma dat zichzelf, net zoals een worm, kan kopiëren. Een virus heeft zich echter altijd in een bestand genesteld, terwijl wormen geen ander bestand nodig hebben. Als een virus een computer is binnengedrongen, zal hij opzoek gaan naar bestanden, om kopieën van zichzelf in die bestanden te laten nestelen. Die bestanden zijn dan geïnfecteerd. Virussen zitten vaak in bijlagen van e-mailtjes of in gedownloade bestanden. De gebruiker van de computer zorgt er dus voor dat het virus op zijn computer terecht komt, ook al weet hij dit zelf misschien niet.

Sommige virussen doen niks anders dan zich verspreiden. Dit kan zeker hinderlijk zijn, omdat de virussen opgeslagen zijn, dus ruimte innemen op de harde schijf (de opslagruimte) van de computer. Verder hinderen ze andere programma's op de computer doordat de virussen zichzelf kopiëren, in plaats van dat de programma's de (rekenkracht van de) computer kunnen gebruiken voor hun taken.

De meeste virussen doen meer dan alleen zichzelf verspreiden, bijvoorbeeld gevoelige gegevens verzamelen en/of verwijderen, of zelfs de controle van de computer overnemen. Deze taken voeren de virussen uit nadat ze zichzelf een aantal keer gekopieerd hebben, het virus wordt dan actief.

Opdracht 28: Worm of virus?

Is de ILOVEYOU worm wel echt een worm of toch een virus? Geef zowel een voor- als tegenargument en trek op basis daarvan een conclusie.

5.5.3 Trojan horse

Een **trojan horse** is een computerprogramma dat zich voordoet als een programma dat je zou willen hebben, bijvoorbeeld een spelletje. In werkelijkheid zorgt een trojan horse er vaak voor dat een crimineel vanaf een andere computer toegang krijgt tot de computer met de trojan horse. Daarnaast kan een trojan horse kan ook zelf schade aanrichten op de computer of gevoelige gegevens verzamelen. Ook kan een trojan horse met de hulp van een virus een computer binnenkomen, waarna hij door het virus naar de computer gekopieerd wordt. Een trojan horse kan zichzelf dus niet kopiëren.

Dat een trojan horse zich voordoet als een leuk of nuttig computerprogramma, maar vervolgens kwaadaardige bedoelingen blijkt te hebben, lijkt erg op de Griekse mythe 'Het paard van Troje'. Vandaar ook de naam trojan horse voor dit type malware. De mythe gaat over een oorlog tussen

de Grieken en de Trojanen. Nadat de Grieken de stad Troje 10 jaar belegerd hebben, bouwen ze een groot houten paard waarin een paar soldaten zich kunnen verbergen. De Grieken doen alsof ze wegvaren, waarna de Trojanen het paard de stad in trekken. s' Nachts kruipen de soldaten uit het paard en openen de poort van de stad. Het Griekse leger is inmiddels terug en kan zo de stad in om Troje in puin te leggen.

Praktijkvoorbeeld: Trojaanse Schimmel

Een tijdje geleden was er een groot bedrijf met een eigen datacentrum, vol gevoelige en strategische gegevens. Het datacentrum werd afgeschermd met:

- sterke fysieke en elektronische beveiligingsmaatregelen
- strikte regels en procedures
- goed getraind personeel

KPMG Amsterdam heeft een afdeling mensen gespecialiseerd in computerbeveiliging. Het bedrijf vroeg KPMG om binnen te dringen in het datacentrum, fysiek of digitaal. Dit binnendringen door 'good guys' wordt ook wel **red teaming** genoemd. Uiteindelijk lukte het ze om als Sinterklaas en Zwarte Piet binnen te komen! Dit is een typisch voorbeeld van **out-of-the-box denken**: zo'n aanval verwacht je niet. Je gaat ervan uit dat Sinterklaas en Zwarte Piet te vertrouwen zijn, Sinterklaas hoeft zich toch niet te identificeren!

Figuur 13: Trojaanse Schimmel

Opdracht 29: Social Engineering

In voorgaande theorie wordt vaak gebruik gemaakt van het manipuleren of voor de gek houden van mensen om bepaalde acties te doen of gevoelige informatie af te geven. Deze manier van manipuleren noemen we ook wel **social Engineering**. Bij welke onderwerpen uit de theorie wordt gebruik gemaakt van social engineering? Beargumenteer je antwoord.

Opdracht 30: Malware schendt security doelen

Welk security doelen worden er geschonden door:

(a) phishing?

(b) een worm die zich alleen maar verspreid?

(c) een virus dat zich alleen maar verspreid?

(d) een trojan horse die een crimineel toegang geeft tot de computer?

(e) malware die bestanden verwijdert?

(f) malware die bestanden vercijfert?

5.6 Jezelf beveiligen

Aangezien je als computergebruiker vaak zelf mee moet werken om malware geïnstalleerd te krijgen of gevoelige gegevens af te staan, helpt het om kritisch na te denken voordat je tot actie overgaat. Daarnaast zijn er ook een aantal maatregelen[4] die je kunt nemen:

1. Gebruik antivirussoftware. Soms is dit niet genoeg om je te beschermen tegen alle soorten malware, en moet je extra programma's installeren. Let op: ook bij het downloaden van antivirussoftware loop je gevaar op malware.
2. Gebruik een firewall. Windows en MacOSX bieden die al aan bij het besturingssysteem.
3. Maak gebruik van aparte gebruikersprofielen/accounts. Niet alle malware kan bij andere gebruikersprofielen naar binnen komen.
4. Update gelijk belangrijke/gevoelige software of laat automatisch updaten. Onder deze software vallen je besturingssysteem, antivirussoftware en je browser.
5. Download software alleen bij de fabrikant.
6. Installeer geen plugins of add-ons van onbekenden.

[4]Gebaseerd op notes van Leo Willems (Copyright leowillems.nl)

6 Privacy

6.1 Anonimiteit

In het hoofdstuk 'Inleiding cybersecurity' is al aan bod gekomen dat authenticatie anders is in de fysieke wereld (het dagelijks leven) als in de digitale wereld. In de fysieke wereld gebruiken we vaak context (informatie uit de omgeving) om vast te stellen met wie we communiceren. In de digitale wereld is die context niet altijd aanwezig. Als je op een website een account aanmaakt met een verzonnen nickname en verder geen informatie over jezelf verstrekt, kun je denken dat je anoniem bent.

"On the Internet, nobody knows you're a dog."

Figuur 14: Anoniem

In werkelijkheid valt die anonimiteit erg tegen, ook als je geen enkele informatie over jezelf beschikbaar stelt. Om verbinding te maken met het internet, gebruikt je computer een uniek nummer: een IP-adres. Dit nummer kan gebruikt worden om al jouw activiteiten op internet te verzamelen. Verder is het ook niet onwaarschijnlijk dat jouw webbrowser uniek is. Webbrowsers verschillen doordat ze verschillende versies hebben, verschillende instellingen en verschillende plugins.

6.2 Profiel

Waarschijnlijk zijn veel van jouw gegevens wel te vinden op internet. Zeker door bedrijven die actief gegevens verzamelen, zoals Google of Apple. Bovendien kunnen gegevens die jij op verschillende plaatsen verstrekt aan elkaar gekoppeld worden als ze overeenkomsten vertonen. Denk aan plaatsen zoals websites, de inbox van je e-mailadressen en cloudservices (waar je gegevens via het internet opslaat op een computer die niet van jou is, bijvoorbeeld Dropbox). Op deze plaatsen worden gegevens verzameld zoals je naam, geboortedatum, adres, telefoonnummer, e-mailadressen, leeftijd, geslacht, burgerservicenummer, bankrekeningnummer, nickname, wachtwoorden, foto's, contacten/vrienden, hoe vaak en wanneer je welke websites bezoekt, waar je veel of weinig op klikt en ander gedrag. Zeker met een combinatie van de genoemde voorbeelden is het mogelijk om precies vast te stellen welke gegevens bij jou horen. Deze gegevens vormen jouw **profiel**, een zo compleet mogelijk beeld van jou, gebaseerd op de gevonden gegevens.

Behalve op het internet, kunnen er ook gegevens verzameld worden van je (mobiele) telefoon. Zeker nu mobiele telefoons ook steeds meer computers worden en je er steeds meer mee kan.

Figuur 15: Toch niet zo anoniem

Je telefoonmaatschappij kan gegevens verzamelen over je bel- en smsgedrag. Als je apps kunt installeren op je mobiel, geef je nog veel meer gegevens af. Grote kans dat apps bijvoorbeeld GPS-data verzamelen, terwijl de app dat zelf niet nodig heeft.

Uit de gegevens die verzameld zijn worden ook dingen afgeleid of voorspeld. Bijvoorbeeld dat als je een meisje bent, je wel interesse hebt in jurkjes of schoenen. Of dat je wel van bier houdt als je veel popfestivals bezoekt. Deze afleidingen en voorspellingen hoeven niet altijd te kloppen met de werkelijkheid. Maar als het juist is, levert het wel extra informatie op die weer gebruikt kan worden.

Meestal worden profielen gebruikt om jou gerichte reclame te laten zien, of om jouw profiel te verkopen. In beide gevallen wordt er dus geld verdiend aan jouw gegevens. Maar de verzamelde gegevens kunnen (in de toekomst) voor veel meer doeleinden worden ingezet. Bijvoorbeeld om jou alleen zoekresultaten te laten zien van dingen die bij jouw profiel horen. Als je iets afwijkends zoekt, kun je dit dus niet vinden. Het beeld dat jij hebt wordt alleen maar bevestigd, de werkelijkheid wordt gekleurd weergegeven. Dit kan erg beperkend en hinderend zijn, wil je niet liever zélf bepalen wat je wel en niet wilt zien? Verder zou je profiel ook gebruikt kunnen worden om te bepalen hoeveel je nog net zou betalen voor een product. Hierdoor wordt er zoveel mogelijk aan jou verdiend. Niet echt eerlijk, als de één meer moet betalen dan de ander voor hetzelfde product.

Opdracht 31: Hoe ziet jouw profiel eruit?

Bepaal met behulp van bovenstaande theorie en onderstaande vragen hoe jouw profiel eruit zou kunnen zien.

(a) Via welke websites, e-mailadressen, cloudservices, telefoonmaatschappij(en) en/of mobiele apps zou informatie over jou verzameld kunnen worden?

(b) Welke gegevens kunnen in jouw profiel zitten? Geef aan hoe zeker je bent dat bepaalde gegevens in je profiel zitten. Zijn er ook gegevens die zeker niet in jouw profiel zitten?

(c) Welke bedrijven hebben een profiel van jou? Hebben ze al jouw gegevens of maar een deel?

6.3 Cookies

Ook als je niet hoeft in te loggen op een website, kan er informatie over je verzameld worden met cookies. Een **cookie** is een klein bestand dat een website op je computer laat opslaan. Dit bestand bevat informatie over de dingen die jij doet op een website. Telkens als je op een website

terugkomt, wordt de informatie in de cookie van de website naar de website opgestuurd. Een cookie mag niet meer dan 255 letters aan inhoud bevatten, maar dit betekent niet dat de website niet meer informatie kan opslaan. Vaak worden er codes gebruikt om informatie kort op te slaan. Ook kan een cookie een klantnummer opslaan. De website slaat dan alle informatie over jou zelf op, waarbij je klantnummer gebruikt wordt om te onthouden over wie de informatie gaat. Telkens als je terugkomt op de website, kan de website verder gaan met informatie verzamelen en het opslaan bij het klantnummer in de cookie.

Soms zijn cookies erg handig. Bijvoorbeeld om te onthouden of een gebruiker ingelogd is of niet en welke gebruiker het is. Hierdoor hoef je niet voor elke pagina die je bezoekt opnieuw in te loggen. Ook kunnen gegevens die je hebt ingevuld in tekstvelden onthouden worden. Deze gegevens zijn dan al ingevuld als je later op dezelfde pagina terugkomt. Verder kunnen persoonlijke instellingen onthouden worden. Bijvoorbeeld een achtergrondkleur, voorkeur voor een taal of welke onderdelen van de website bovenaan moeten staan. Dit soort **functionele cookies** maken het dus mogelijk dat je de website (beter) kunt gebruiken.

Behalve functionele cookies zijn er ook cookies die enkel als doel hebben om informatie over jou te verzamelen. Dit zijn **tracking cookies**, ofwel cookies die volgen wat jij allemaal doet op een website. Zo wordt zoveel mogelijk informatie over jou verzameld, waarmee een profiel van jou gemaakt wordt. Dit profiel kan vervolgens ingezet worden voor doeleinden zoals hierboven besproken zijn.

Sommige websites laten inhoud zien van andere websites. Vaak zijn dit reclameadvertenties of like-buttons. Die andere websites, die getoond worden op de webiste die jij bezoekt, mogen ook cookies opslaan op jouw computer. Dit soort cookies worden **third-party cookies**. genoemd. Als een website reclame, like-buttons of andere inhoud mag tonen op verschillende websites, kan de third-party cookie op al die verschillende websites informatie over jou verzamelen.

Figuur 16: Facebook like-button

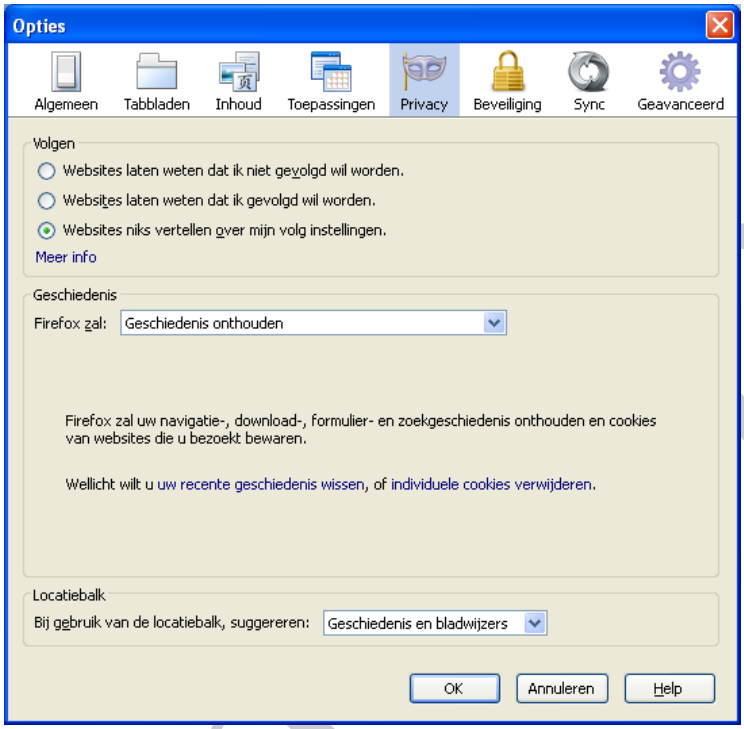
Opdracht 32: Cookies verwijderen in Firefox

(a) Klik in het 'Extra'-menu op 'Opties'. Klik vervolgens op het tabblad 'Privacy'. Bovenaan kun je kiezen of je wilt dat Firefox aan websites laat weten of je gevolgd wil worden (met cookies), of dat je websites niks wil laten weten. Websites kunnen echter nog steeds tracking cookies plaatsen als Firefox aan websites laat weten dat je niet gevolgd wilt worden.

(b) Klik nu op 'individuele cookies verwijderen'. Je krijgt nu een lijst te zien met al je cookies. Zoek drie cookies van websites die je kent en drie van websites die je niet kent. Heb je ook een cookie van de website van je school?

(c) Kies een interessante cookie. Klik op het '+'-teken en een cookie die nu verschijnt. Hoogstwaarschijnlijk zie je bij 'Inhoud' een aantal cijfers met punten ertussen, dus een code of klantnummer. Bij 'Domein' zie je van welke website de cookie afkostig is. Bij 'Verloopt' staan de datum en tijd waarop de cookie weggegooid wordt. Noteer van deze cookie wat er staat bij 'Domein' en 'Verloopt'.

(d) Kies nu een cookie die je wilt verwijderen. Selecteer een enkele cookie of de hele map. Klik nu op 'Cookie verwijderen' om de cookie(s) te verwijderen. Ga nu naar de website waarvan je de cookie verwijderd hebt. Staat er nu weer een cookie van die website in de lijst? Misschien vraagt de website nu wel om toestemming om cookies te plaatsen, er zijn immers geen cookies meer te vinden op je computer.



Figuur 17: Privacy instellingen van Firefox

Figuur 18: Lijst met cookies

Opdracht 33: De cookies die je krijgt terwijl je surft

(a) Collusion is een add-on voor Firefox waarmee je kan zien welke cookies je krijgt als je naar een website gaat. Ga in het 'Extra'-menu naar 'Add-ons'. Zoek de add-on Collusion op met de zoekbalk. Klik op 'Meer' om informatie te krijgen. Als je ziet dat de add-on van http://www.mozilla.org komt, dan is deze add-on te vertrouwen en kun je op 'Installeren' klikken.

(b) Klik op 'Collusion Graph' in het 'Extra'-menu. Als het goed is zie je alleen een menuutje aan de linkerkant en voor de rest een zwart scherm. Zo niet, klik dan op 'Reset' in het menu.

(c) Ga nu (in een andere tab) naar ah.nl, nu.nl, youtube.nl en nos.nl. In de Collusion-tab verschijnen nu bolletjes met lijnen ertussen. Elk bolletje is een website. De lichtgevende bolletjes zijn de websites waar je geweest bent. De bolletjes waarmee de lichtgevende bolletjes verbonden zijn (met een lijntje), zijn de websites die jou volgen met third-party cookies.

(d) Probeer nu zelf een paar websites. Welke website is met de meeste websites verbonden? Kun je ook een website vinden die geen third-party cookies heeft?

6.4 Sociale media

Sociale media zijn er in allerlei soorten: om contact te houden met vrienden of zakelijke contacten, over bepaalde interesses of hobby's, voor dating en om dingen te melden over je hele leven. Sociale media kunnen erg leuk en handig zijn. Maar bedenk wel dat alle informatie die je beschikbaar stelt, gebruikt kan worden. Sociale media zijn vaak gratis, maar dat betekent niet dat ze niets aan jou verdienen. Sociale media zijn bij uitstek verzamelaars van gegevens waarmee ze profielen kunnen maken. Met deze profielen kunnen ze gerichte advertenties tonen, ze kunnen de profielen doorverkopen en wie weet wat ze in de toekomst nog verzinnen. Ook andere partijen kunnen hun voordeel doen met al die gegevens op sociale media. Bijvoorbeeld als je gaat solliciteren of een verzekering wil afsluiten. Of voor dieven die een bezoekje brengen aan je huis terwijl je op vakantie bent.

Het is dus belangrijk om goed na te denken over de gegevens die je beschikbaar stelt. Een foto kan nu wel grappig zijn, maar denk je daar over een paar jaar net zo over? En maak vrienden duidelijk welke gegevens ze wel en niet over jou online mogen zetten. Als sociale media privacy instellingen aanbieden, gebruik deze dan. Maar bedenk dat sociale media, ook als je account helemaal is afgeschermd, kunnen zien wat erop staat. Verder is het erg moeilijk om gegevens verwijderd te krijgen, op internet kan het altijd wel weer ergens opduiken. Als je iets moet invullen wat je niet kwijt wilt, verzin dan iets. Anderen kunnen dit ook, of gaan misschien zelfs verder door zich beter voor te doen dan ze in werkelijkheid zijn. In het algemeen geldt: blijf kritisch nadenken.

Figuur 19: Sociale media

Opdracht 34: Sociale media

(a) Noem van elk van de genoemde soorten van sociale media een voorbeeld.

(b) Welke social media gebruik jij? Onder welke soort vallen ze, of zijn er nog andere soorten?

(c) Heb je wel eens iets online gezet, waar je later niet meer zo blij mee was? Is je gedrag hierdoor veranderd?

(d) Welke gegevens zet je (expres) niet online en welke wel?

(e) Denk je dat sociale media veel over je weten? Beargumenteer je antwoord.