MODULE

Cybersecurity

Ontwikkeld door:
Petra van den Bos

Onder begeleiding van:
Erik Poll
Marko van Eekelen

Gecertificeerd als NLT module vanaf:
Februari 2017

Email: module-cybersecurity@cs.ru.nl

Website: `http://module-cybersecurity.cs.ru.nl`

16 maart 2017

RADBOUD UNIVERSITEIT

Colofon

De module Cybersecurity is bestemd voor de lessen Natuur, Leven en Technologie (NLT). Versie 1.0 van de module is op 31 januari 2017 gecertificeerd door de certificeringscommissie van de Vereniging NLT onder nummer X239-084-VE1-F1.

De module is ontwikkeld door Petra van den Bos, MSc., Prof. dr. Marko van Eekelen en Dr. Erik Poll werkzaam bij de Digital Security groep van de Radboud Universiteit Nijmegen.

Aangepaste versies van deze module mogen alleen verspreid worden indien in dit colofon vermeld wordt dat het een aangepaste versie betreft, onder vermelding van de naam van de auteur van de wijzigingen.

Over de auteurs

Petra van den Bos is Master-studente Informatica aan de Radboud Universiteit in Nijmegen. Prof.dr. Marko van Eekelen en dr. Erik Poll werken aan de Radboud Universiteit in de Digital Security groep, waar ze onderzoek doen en onderwijs gegeven op gebied van cybersecurity.

De Digital Security groep is de grootste onderzoeksgroep op gebied van cybersecurity in Nederland, en onderzoek van de groep heeft geregeld het nieuws gehaald (o.a. door het kraken van de ov-chipkaart en onderzoek naar digitale beveiliging van bijv. auto's en internetbankieren). De groep verzorgt een Bachelor opleiding Cybersecurity aan de Radboud Universiteit als specialisatie binnen Informatica (zie `http://www.ru.nl/cybersecurity`).

Leerdoelen

In deze module leer je:

- te beargumenteren welke securitydoelen relevant zijn in een praktijksituatie.
- wat het verschil is tussen de begrippen identificatie, authenticatie en autorisatie en kun je aangeven welke begrippen wel/niet van toepassing zijn in praktijksituaties.
- basistechnieken voor symmetrische cryptografie toe te toepassen om berichten te vercijferen en ontcijferen.
- hoe asymmetrische cryptografie toegepast wordt bij internetbeveiliging.
- protocollen, die asymmetrische cryptografie gebruiken, te begrijpen en om kwetsbaarheden erin aan te wijzen en te verbeteren.
- verschillende soorten digitale gevaren te herkennen en te benoemen.
- met een kritische blik te kijken naar de privacyrisico's die je loopt in je dagelijks leven.

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 rapportcijfers in de administratie van een school of medische gegevens op een computer bij een huisarts of ziekenhuis. Bij digitale diensten kun je denken aan internetbankieren, Gmail en Facebook. Uiteindelijk gaan dergelijk diensten over het lezen of wijzigen van digitale gegevens: de gegevens over je bankrekening (inclusief hoeveel geld je hebt!), al je emails, of de inhoud van je Facebook pagina. Het 'cyber' in cybersecurity benadrukt extra dat het gaat om security in cyberspace, de virtuele wereld van die bestaat uit computers en netwerken tussen computers.

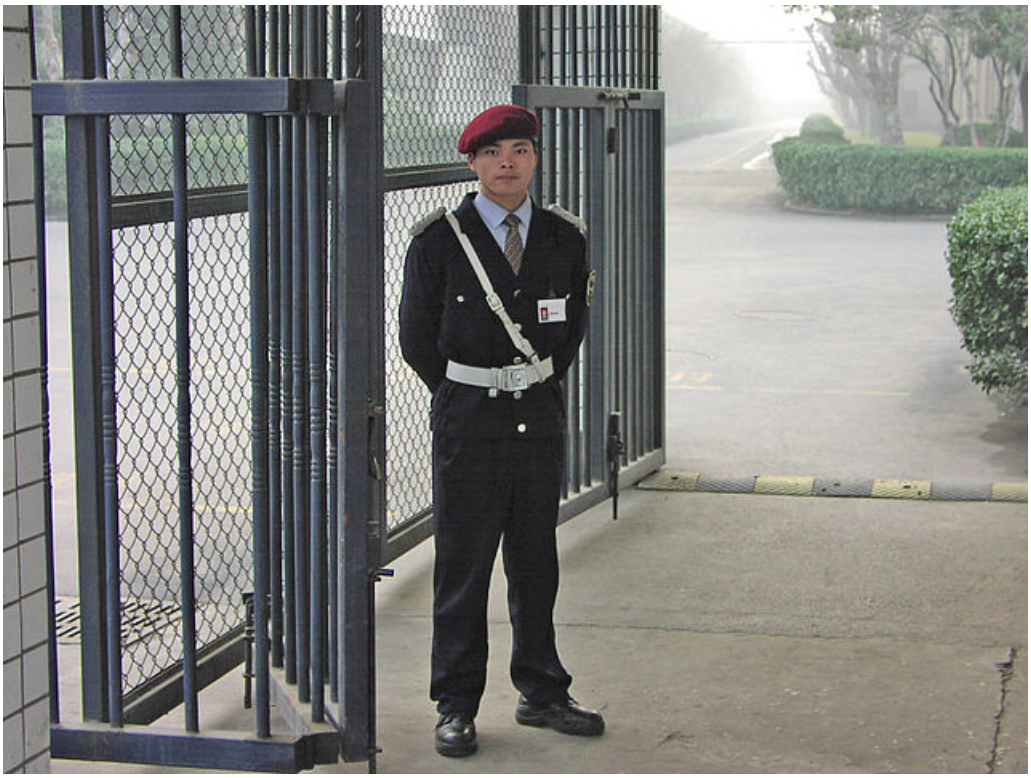
Digitale informatie kan beschermd worden met **cryptografie**. Meer hierover volgt in de hoofdstukken 'Symmetrische cryptografie' en 'Asymmetrische cryptografie'.

Digitale diensten worden vaak beschermd door een vorm van **toegangscontrole**, di ervoor zorgt dat alleen bepaalde mensen toegang hebben. Bijvoorbeeld, het is de bedoeling dat alleen jij toegang hebt tot je gmail account, en alleen jij dus email naar deze account kan lezen en email vanaf dit account kan sturen. Voor je Facebook account is het de bedoeling dat jij informatie op je pagina kan veranderen of toevoegen, maar anderen (bijvoorbeeld je Facebook friends) kunnen deze informatie mogelijk wel lezen. Deze toegangscontrole wordt gedaan met software: de software op de servers van Google en Facebook bewaakt de toegang tot je gmail account en je Facebook pagina. De software vraagt je bijvoorbeeld om je username en wachtwoord in te voeren, en alleen als deze kloppen geeft de software je toegang tot diensten zoals bijvoorbeeld het lezen en versturen van email. Toegangscontrole wordt uitgebreider behandeld in het hoofdstuk 'Authenticatie'.

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**.

Beveiliging is nooit perfekt: een aanvaller met genoeg kennis, geld, tijd, geduld en creativiteit kan vrijwel elke beveiliging doorbreken. Bijvoorbeeld, een aanvaller die de email op jouw gmail account wil lezen kan alle mogelijke wachtwoorden gaan zitten uit te proberen (als de aanvaller erg veel tijd en geduld heeft), bij je thuis inbreken en een camera installeren om je wachtwoord af te kijken, bij Google inbreken, of gewoon het bedrijf Google opkopen en dan je email op de servers lezen (als de aanvaller erg rijk is). Maar dit zijn waarschijnlijk niet de meest realistische aanvallen. Het is waarschijnlijk een groter risico dat de aanvaller met een phishing email je wachtwoord probeert te achterhalen, of dat een aanvaller digitaal inbreekt op je computer om daar je wachtwoord te achterhalen.

Uiteindelijk moet er bij de beveiliging een afweging gedaan worden van risico's: we moeten een afweging maken tussen de schade die een aanvaller kan aanrichten en de kosten en moeite die we in de beveiliging steken. Om deze afweging te maken moeten we ook een inschatting maken van wat de



Figuur 1.1: Toegangscontrole [Foto door Robbie Sproule]

aanvaller allemaal kan, en hoeveel kennis, tijd, hulpmiddelen en geld de aanvaller heeft, Met andere woorden: *wat* willen we beschermen, *tegen wie*, en *hoeveel mag de beveiliging kosten*.

De begrippen **beveiliging** en **veiligheid** worden nog al eens door elkaar gehaald. Beide begrippen gaan allebei over bescherming, maar **beveiliging** gaat over de bescherming tegen een actieve aanvaller, die doelbewust toegang probeert te krijgen tot het systeem. Bij **veiligheid** is er geen actieve aanvaller, maar gaat het om bescherming tegen ongelukken en dingen die per ongeluk fout kunnen gaan. Dus als we een vliegtuig proberen te beschermen tegen terroristen die het willen kapen of opblazen dan gaat het om beveiliging, als er een vliegtuig proberen te beschermen tegen blikseminslag of een mechanische storing in een van de motoren dan gaat het om veiligheid.

De Engelse termen hiervoor zijn **security** en **safety**. Bij cybersecurity gaat het dus om beveiliging en niet om veiligheid.

Opdracht 1 **Indringer**

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

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

(b) Om welke digitale informatie ging het? Wat is er met die informatie gebeurd? 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 en zijn de toehoorders de ontvangers. Wat je zegt is de inhoud van het bericht. De lucht is het medium, want daar gaat het geluid van je stem doorheen voordat het de ontvangers bereikt.

Figuur 1.2: Een bericht

Soms zijn er ook onbedoelde ontvangers van het bericht, omdat die ontvangers per ongeluk of expres meeluisteren. Bijvoorbeeld als je een gesprek hoort in de trein omdat je in de buurt zit, of als iemand stiekem door de deur heen een gesprek afluistert. In de digitale wereld is het zelfs vrij makkelijk om berichten aan te passen voordat ze bij de ontvangers aankomen. Als je met elkaar praat is dit moeilijker. Iemand kan dan alleen het bericht veranderen door er hard door heen te schreeuwen zodat de gesprekspartners elkaar niet verstaan. Oorspronkelijk hoorde de een wat de ander zei, nu hoort hij alleen geschreeuw, dus is het bericht veranderd van wat er gezegd werd naar wat de verstoorder schreeuwt.

Om uit elkaar te houden wie goede en wie kwade bedoelingen heeft, wordt er in de security vaak gesproken over bepaalde personages. Alice en Bob zijn de ‘good guys’. Zij sturen elkaar berichten. Eve (van ‘evil’ of ’eavesdropping’) 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) Bekijk het plaatje in figuur 1.2. Wie is de zender van het bericht? Wie zijn de ontvangers? Wat is de inhoud? Welk medium wordt gebruikt?

(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 Securitydoelen

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 ze zomaar kan lezen: we willen dat deze digitale informatie vertrouwelijk blijft. Denk bijvoorbeeld aan medische gegevens, geheime staatsinformatie, militaire informatie, informatie die de politie heeft over verdachten en criminelen, maar ook informatie die criminelen hebben en waarvan ze niet willen dat de politie âĂŞ of concurrerende criminelen âĂŞ 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 vertrouwelijk zijn: denk maar aan je pincode of je wachtwoord, al je sms'jes, e-mails en skype-berichten.

  Privacy is een bijzonder geval van vertrouwelijkheid en wordt gebruikt als het over de vertrouwelijkheid van privégegevens gaat. Denk bijvoorbeeld aan medische gegevens, financiële gegevens over bijvoorbeeld je bankrekening, 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 er bijvoorbeeld verkeerde informatie over iemands bloedgroep of allergieën in dossiers terecht komt, kan dat 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-aanvallen (DoS staat voor Denial of Service). We zullen ze uitgebreider bespreken in het hoofdstuk 'Digitale gevaren'.

De beveiligingseis die hiermee geschonden wordt is de beschikbaarheid van de 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. Je kunt bijvoorbeeld een DoS-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. Als de klanten al binnen zijn kunnen ze niet bij de kassa of uitgang komen. Het uitvoeren van zo'n aanval 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 nodig, want je kunt de boel automatiseren. Duizenden virtuele klanten kunnen dan een webwinkel bezoeken om de website te laten vastlopen.

- **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: meestal is in één oogopslag duidelijk om wie het gaat. Je ID-kaart 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-kaart 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 je in het ziekenhuis een man ziet in een witte jas, wat denk je dan? Dat zal wel een dokter zijn. En als je een vrouw ziet in een witte jas? Dat zal wel een verpleegster zijn. Misschien is het dan verrassend 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 afgelegen 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 dat suggereert dat je met een echte pinautomaat te maken hebt.

  In de digitale wereld is er vaak minder (duidelijke) context 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 het hoofdstuk 'Authenticatie' volgt meer hierover.

- **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 gegaan. 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 op papier, is er ook wetgeving over het gebruik van handtekeningen in de digitale wereld. Een belangrijke manier om onweerlegbaarheid te realiseren is het gebruik van digitale handtekeningen, al zijn digitale handtekeningen 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, zeker als er geen getuigen zijn. Op websites moet je soms aanvinken dat je akkoord gaat met de gebruiksvoorwaarden voor je naar de volgende pagina kan. Hiermee

Figuur 1.3: Een overeenkomst tussen de ministers van Buitenlandse Zaken van Nederland en Duitsland – onweerlegbaar dankzij de handtekeningen én de getuigen, én de foto die ervan gemaakt is.

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 om te zorgen dat kopers ergens mee akkoord gaan, valt te betwisten.

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 betrouwbaar is.

Opdracht 3 Cijferadministratie

Welke securitydoelen 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. Beargumenteer je antwoord met voorbeelden.

Opdracht 4 Welk securitydoel?

Welk securitydoel 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 hersteld 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-alike steelt jouw ID-kaart. Vervolgens fietst hij zonder licht. Hij wordt aangehouden en laat jouw ID-kaart zien aan de agent. Hierdoor krijg jij een boete thuisgestuurd.

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

(f) Een look-alike leest stiekem de vingerafdrukken op jouw ID-kaart 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 Authenticatie

2.1 Identificatie 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-kaart 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 5 **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.

(c) De streepjescode van een supermarktproduct.

Figuur 2.1: Nummerplaat

2.2 Autorisatie

Als je inlogt op een webpagina heb je vaak een aantal 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 ingelogd 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.

2.3 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 een 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 op jouw naam. 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. We vatten het woord 'computer' hierbij heel breed op, waardoor bijvoorbeeld een auto of pinautomaat ook computers zijn. Je kunt je authenticeren aan een computer:

- met **iets wat je hebt**, dus een voorwerp. Bijvoorbeeld een (elektronische) autosleutel of een bankpas.
- met **iets wat je bent**, dus een kenmerk dat 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.

Figuur 2.2: Een uniek biometrisch kenmerk: de vingerafdruk

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. Alle 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 heeft. 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 6 **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 je ID-kaart.

(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.

2.4 Veilige wachtwoorden

De meeste wachtwoorden die mensen kiezen zullen niet bestand zijn tegen een brute-force-aanval (waarbij de aanvaller de beschikking heeft over zoveel computers als nodig). Onderzoek wijst uit dat een wachtwoord pas écht hélemaal veilig is 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 beschermt 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.

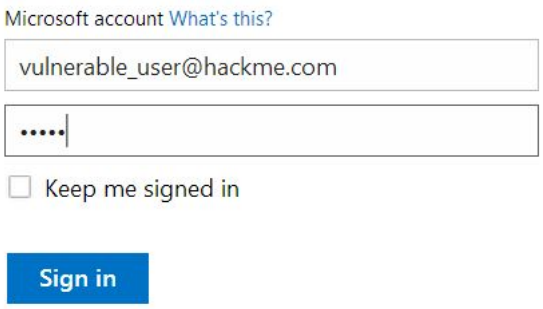
2.5 Richtlijnen

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 hetzelfde wachtwoord op verschillende websites gebruikt, kan een aanvaller met die loginnamen gelijk op al die websites inloggen.

[1] Copyright leowillems.nl

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 in een documentje op je computer of mobiel.



Figuur 2.3: Zwak wachtwoord

Opdracht 7 **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?

2.6 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 soms een captcha invullen als je een account aanmaakt (op een website), bijvoorbeeld bij het aanmaken van een Gmailaccount.

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.

(a) Vorm groepjes van twee. Maak 3 captcha's voor de ander:

(i) Een captcha die een computer ook nog wel kan herkennen.

Figuur 2.4: Captcha's

(ii) Een captcha die een mens nog wel kan herkennen maar een computer niet.

(iii) Een captcha die alleen jij kan herkennen, dus de ander niet.

Laat de ander je captcha's lezen. Lukt dat bij allemaal?

(b) Vergelijk je eigen captcha's met die op Internet.

(i) Lijkt je tweede captcha op de captcha's op Internet?

(ii) Zijn er captcha's die meer op je eerste of derde captcha lijken?

(iii) Welke technieken worden gebruikt om de letters moeilijk te maken voor de computer? Kun je je eigen captcha's nog moeilijker maken met deze technieken?

Opdracht 8 **Captcha's maken**

2.7 Praktijkvoorbeeld: Authenticatie in mobiele telefonie

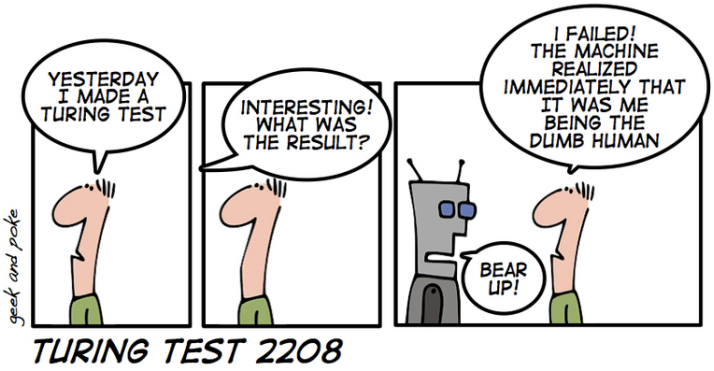
Wanneer je belt met je mobiele telefoon betaal je voor dat gesprek. Dit maakt het belangrijk dat je provider zeker weet dat jij dat gesprek voert, dus is wederom authenticatie nodig!

Mobiele telefoons gebruiken SIM (Subscriber Identification Module) kaarten voor de authenticatie. Deze SIM kaarten bevatten een uniek serienummer (voor identificatie) en een geheim (voor authenticatie), die allebei ook bekend zijn bij de provider.

Wanneer een GSM telefoon wordt aangezet, dan stuurt hij eerst het unieke serienummer van de SIM door. De zendmast van de provider wil dan weten of dit serienummer van een echte SIM af komt, of van een aanvaller. De zendmast zou dit kunnen testen door te vragen om het geheim dat alleen hij en de SIM kennen, maar als een aanvaller meeluistert, dan weet hij vanaf dat moment ook het geheim! Om dat probleem te voorkomen gebruiken de zendmast en SIM kaart een speciale truc. In plaats van rechtstreeks te vragen om het geheim, stelt de zendmast een vraag waarbij het geheim nodig is om het correcte antwoord te geven, maar het geheim zelf niet in het antwoord zit. Je kunt je dit voorstellen als dat beide partijen een boek kiezen en dat de zendmast iedere keer vraagt om het zoveelste woord van een bepaalde pagina. Alleen iemand met hetzelfde boek kan dan het juiste antwoord geven. Het is dan wel heel belangrijk dat de zendmast iedere keer een andere vraag stelt, anders kan een aanvaller simpelweg een eerder antwoord herhalen! Deze methode wordt 'challenge-response', oftewel vraag-en-antwoord genoemd, omdat bij iedere authenticatie de SIM opnieuw wordt uitgedaagd om zijn identiteit te bewijzen.

Toch zit er nog steeds een beveiligingsprobleem in deze authenticatie. Zie jij het probleem?

Als je goed kijkt, dan zie je dat de telefoon zich authenticeert naar de zendmast toe, maar de zendmast hoeft dit niet te doen naar de telefoon toe. Dit betekent dat een aanvaller zich voor zou



[Bron: Oliver Widder, `http://geek-and-poke.com`]

kunnen doen als een zendmast, zonder dat de telefoon of SIM dit merken! Door het op deze manier afgeluisterde serienummer te sturen naar een echte zendmast, kan de aanvaller net doen of hij de echte telefoon is. De echte zendmast vraagt dan aan de aanvaller om te bewijzen dat hij de juiste SIM kaart heeft, maar de aanvaller kan deze vraag doorsturen naar de echte SIM kaart. De echte SIM kaart zal vervolgens het juiste antwoord geven, omdat hij denkt dat de aanvaller een echte zendmast is en de aanvaller kan op zijn beurt het goede antwoord doorsturen naar de echte zendmast. Vanaf dat moment lijkt het voor de echte zendmast alsof hij praat met de echte telefoon en andersom, maar in werkelijkheid praten ze beiden tegen de aanvaller.

Om dit probleem op te lossen moet in moderne mobiele telefonie de zendmast zich eerst authenticeren naar de SIM kaart toe. Zo weet de SIM kaart zeker dat hij tegen een echte zendmast praat en kan hij zonder problemen antwoord geven op vragen van de zendmast. We spreken hier ook wel van wederzijdse authenticatie.

Deze oude en nieuwe manier van authenticatie worden nog steeds door elkaar heen gebruikt. Bij de meeste mobiele telefoons kun je zien welke methode op dit moment door je telefoon wordt gebruikte: als je telefoon GSM of GPRS gebruikt, meestal aangegeven door een ‘G’ in beeld, dan gebruik je op de moment alleen de enkelzijdige authenticatie. De modernere varianten, vaak aangegeven door een ‘U,’ een ‘H,’ een ‘H+’ of een ‘L’ in beeld, gebruiken de wederzijdse authenticatie en zijn dus veiliger.

3 Symmetrische cryptografie

3.1 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** ofwel **versleutelingstechniek** 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.

3.2 Scytale

De Oude Grieken verstuurden al geheime berichten, bijvoorbeeld met de **scytale** ($\sigma\kappa\upsilon\tau\alpha\lambda\eta$). Dat is een cilindervormig stuk hout. Om een bericht te vercijferen rolden ze een lange smalle strook papier (of eigenlijk papyrus in die tijd) om de scytale, waarbij alle stroken precies naast elkaar op de rol te zien waren. Vervolgens schreven ze van links naar rechts je boodschap op, waardoor op de (uitgerolde) strook telkens een stuk werd overgeslagen. De letters op de strook staan hierdoor 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 zender.

Figuur 3.1: Scytale

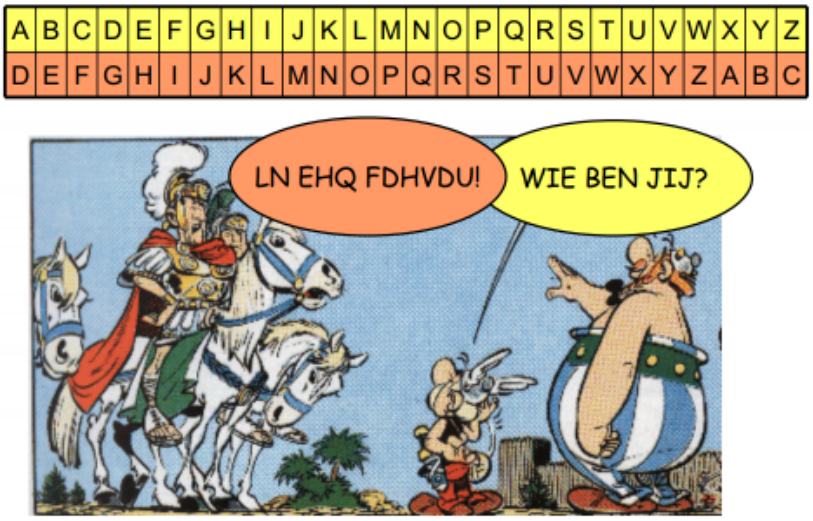
De strook kon door een willekeurige boodschapper vervoerd worden, want de strook bevatte geen

leesbaar bericht. In de security gaan we er altijd van uit dat iedereen het (onleesbare) bericht kan zien als 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.

3.3 Caesarversleuteling

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 vertaald 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.



Figuur 3.2: Caesarversleuteling

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 caesarversleuteling 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. Dit is bijvoorbeeld het geval als er maar één sleutel is, of als je de sleutels kan achterhalen als je weet wat het algoritme is. Als in zo'n geval het algoritme 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. Een voordeel van het openbaar maken van het algoritme 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 het algoritme, alleen van de geheimhouding van de sleutel, wordt het **het principe van Kerckhoffs**

genoemd. Auguste Kerckhoffs is bekend om dit principe, vandaar de naam. Bij een website waarop je moet inloggen mag je dus best weten dat je alleen binnenkomt als je een loginnaam en bijbehorend wachtwoord hebt. Maar je wachtwoord moet je wel geheim houden.

3.4 Symmetrische cryptografie

Bij symmetrische cryptografie wordt bij het versleutelen en het ontsleutelen dezelfde sleutel gebruikt. Dit betekent dus de zender en de ontvanger die geheime berichten willen uitwisselen dezelfde sleutel moeten hebben. Als er meerdere zenders en ontvangers zijn, dan zouden deze allemaal dezelfde sleutel kunnen gebruiken, maar het is veiliger als er voor elke combinatie van zender en ontvanger een unieke sleutel is die alleen deze zender en ontvanger hebben: dan kunnen ze namelijk zeker weten dat alleen zij tweeën de berichten kunnen lezen die ze uitwisselen.

Met cryptografie kun je behalve het doel vertrouwelijkheid ook andere securitydoelen 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 is. Dit komt doordat de aanvaller de sleutel niet heeft. Hierdoor kan hij geen vercijferde tekst maken die na ontcijferen met de juiste sleutel weer leesbaar is. Hij zou kunnen proberen te gokken, maar bij een veilige versleutelingstechniek is er een verwaarloosbaar kleine kans op een leesbaar stuk tekst na ontcijferen van het gegokte stuk vercijferde tekst.

Niet alle methodes om een bericht te vercijferen en ontcijferen zijn even veilig. Een methode is onveilig als je de sleutel die gebruikt is makkelijk kan, waardoor je het bericht kan ontcijferen. Als je een vercijferd bericht kan ontcijferen zonder dat je de sleutel weet zeggen we ook wel dat je 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. Uiteindelijk is elke versleuteling met een brute-force-aanval te kraken, maar de vraag is hoeveel mogelijke sleutels er zijn, en hoeveel tijd je het kost om ze allemaal uit te proberen. 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.

Bij de caesarversleuteling is een brute-force-aanval 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 versleutelingstechnieken voor. Als je een sleutel kiest moet je dus altijd controleren of het geen triviale sleutel is.

Opdracht 9 **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 kartonnen kokers van keukenrollen en (aan elkaar geplakte) stroken papier om je buurman een geheim bericht te sturen.

(e) Probeer nu zonder koker het bericht van je buurman te ontcijferen. Gebruik dat je al weet wat de eerste twee letters van het bericht zijn (je hebt net het hele bericht gezien, maar doe net alsof je alleen de eerste twee letters weet). 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?

3.5 Substitutie en transpositie

Bij een **substitutieversleuteling** wordt elke letter van het oorspronkelijke bericht vertaald 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.

Een caesarversleuteling is ook een substitutieversleuteling. Je vertaalt dan ook iedere letter naar een (andere) letter. Bij een caesarversleuteling staan de vertalingen van twee opvolgende letters van het alfabet ook na elkaar in het alfabet. Bij een substitutieversleuteling hoeft dat niet altijd zo te zijn, 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. Je zou bijvoorbeeld een bericht achterstevoren kunnen schrijven, raam tad si kjilekkam et nedar roov nee rellavnaa. Dit moet je het doorelkaarhusselen wel systematisch doen, anders kun je het oorspronkelijke bericht niet achterhalen uit het vercijferde bericht. Hiervoor kun je bijvoorbeeld een bericht eerst in een aantal blokken met ieder hetzelfde aantal letters verdelen. 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. Bijvoorbeeld, 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 worden dus op dezelfde manier door elkaar gehutseld. De nieuwe blokken plak je gewoon weer achter elkaar.

Om het bericht 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 hoe vaak een tekst gemiddeld die letter bevat. 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 de vercijferde tekst veel (of juist weinig) bevat, kun je met de letterfrequentie bepalen wat de oorspronkelijke letters zijn die vercijferd zijn naar die veel (of weinig) voorkomende letters.

Opdracht 10 **Transpositieversleuteling**

Vorm tweetallen. Jullie gaan elkaar een geheim bericht sturen.

(a) Verzin allebei 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) Bij (b) staat beschreven hoe je een bericht vercijfert. Schrijf nu (samen) op hoe je een (vercijferd) bericht weer ontcijfert, dus hoe je de letters moet verplaatsen om het bericht weer leesbaar te

maken.

(d) Ontcijfer elkaars vercijferde bericht. Klopt de ontcijfering met het originele bericht?

Opdracht 11 Caesarversleuteling

Hieronder staan caesarversleutelingen. Probeer de sleutel, dus hoeveel 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

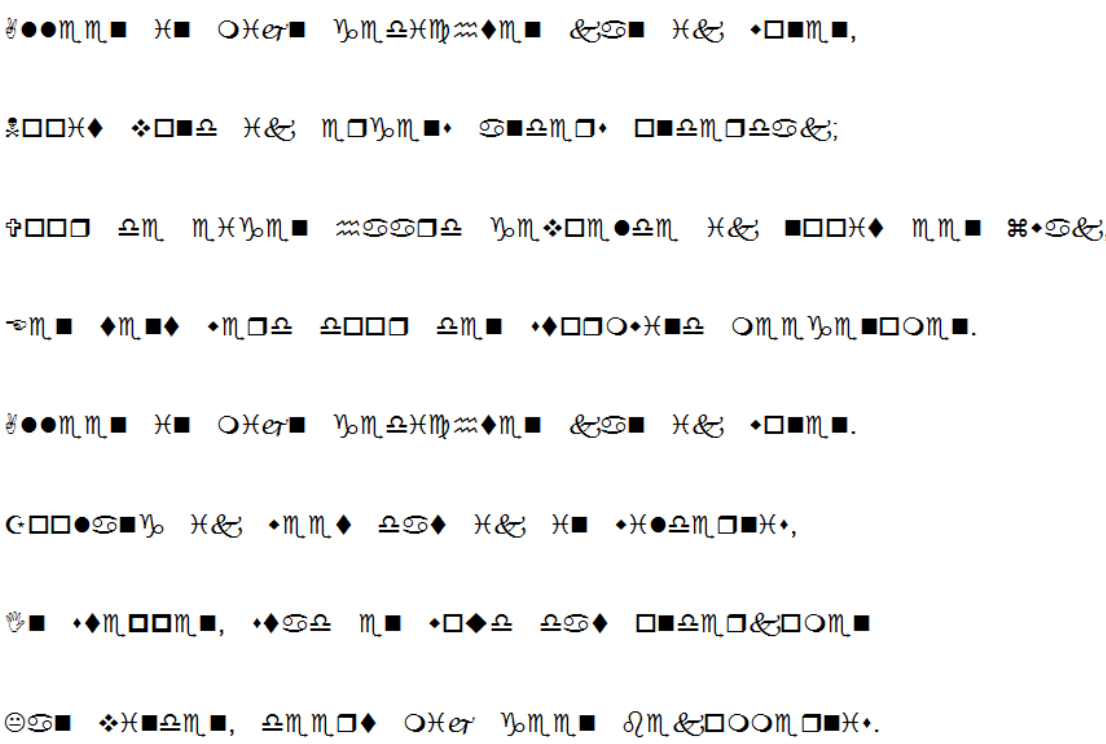
(b) VJJAJUBMNJVNNAEXXATXVCMJWFXAMCQNCUJBCRP

Opdracht 12 Substitutie of transpositie?

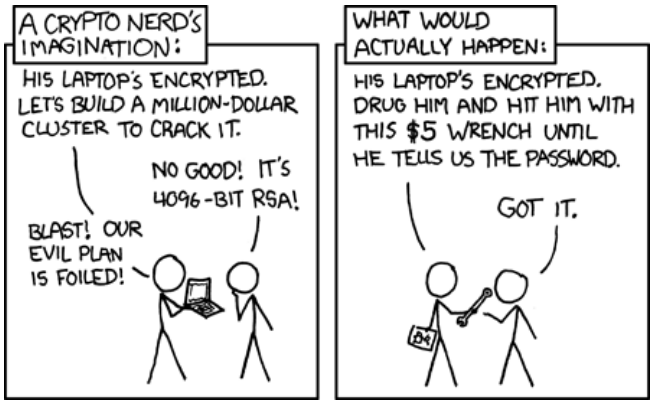
Bepaal met behulp van de letterfrequentie of het volgende bericht een substitutieversleuteling of een transpositieversleuteling is:
OIDZUBIRTEHEECTSSBNUITUTTEJIICEFOFROEHTCNARE
TSSONPTCEIIJREIFIANZJSDELJTNUIKLEZTEWTENEETEJH

Opdracht 13 Monoalfabetische substitutie

In figuur 3.3 staat een tekst die versleuteld is met een zogenaamde monoalfabetische versleuteling. Hierbij is voor elke letter een symbool gekozen, en zijn alle voorkomens van die letter vervangen door dit symbool. Probeer het te ontcijferen door bij elk symbool de bijbehorende letter te vinden. De spaties, komma's en punten staan op de juiste plaats. Zoek de Nederlandse letterfrequentie op en maak hiervan gebruik om de eerste letters te vinden.



Figuur 3.3: Substitutieversleuteling



Figuur 3.4: Vaak is de versleuteling niet de zwakste schakel in de beveiliging ...[xkcd.com]

Opdracht 14 Veilig

Welke versleutelingstechniek is moeilijker om te kraken, de caesarversleuteling of de monoalfabetische substitutie uit opdracht 3.5? Beargumenteer je antwoord. Denk hierbij aan het aantal sleutels dat je kunt kiezen bij de twee versleutelingstechnieken. Waarom maakt het uit hoeveel het er zijn?

3.6 Moderne versleutelingstechnieken

Voorgaande versleutelingstechnieken waren allemaal niet erg veilig. Zeker met de hulp van een computer kun je de sleutel achterhalen. Hierdoor kun je de originele berichten achterhalen zonder dat je van tevoren wist wat de sleutel was. Moderne versleutelingstechnieken zijn meestal een stuk ingewikkelder en veiliger. De eerste moderne versleutelingstechniek 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, ofwel de geheime dienst) 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 reden 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 dat ze juist goed bestand waren tegen aanvallen.

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 er tekst vercijferd en ontcijferd werd. Ten derde moest het onmogelijk zijn om de methode te kraken als je wel wist hoe het algoritme werkte maar niet welke sleutel gebruikt was (volgens het principe van Kerckhoffs). 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.

4 Asymmetrische cryptografie

4.1 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 één 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) = $\frac{1}{2}n^2$- $\frac{1}{2}$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, staat 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

4.2 Asymmetrische cryptografie

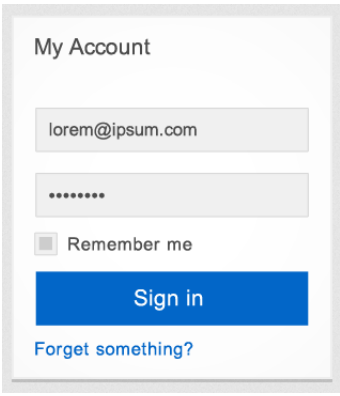
Asymmetrische cryptografie biedt een oplossing voor het grote aantal sleutels dat nodig is bij symmetrische cryptografie. We zullen hier een analogie uitleggen zodat je je (hopelijk) beter een beeld kunt vormen bij deze techniek. Ieder persoon heeft een sleutel en een heel stel (hang)sloten die geopend 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 **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**.

De zender 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. De ontvanger 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 vercijferd heeft met het slot.

4.3 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**.



Figuur 4.1: Inloggen

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 haar 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. Daarom kunnen deze gegevens beter vercijferd over het internet gestuurd worden. 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: het doel was juist om niet zo veel verschillende sleutels en sloten nodig te hebben. Als Alice's gebruikersnaam en wachtwoord vercijferd over het internet gaan kan Eve ze afluisteren. Later kan Eve ze dan opnieuw sturen, waardoor het haar lukt om in te loggen als Alice. Het vercijferen van Alice's gebruikersnaam en wachtwoord heeft dus niet geholpen om te voorkomen dat Eve als Alice kan inloggen.

Opdracht 15 Securitydoelen bij inloggen op webpagina

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

4.4 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 er vanuit dat alles wat ze van Trent krijgen klopt. Je zou Trent kunnen vergelijken met een notaris. Trent wordt ook wel 'Trusted Third Party' genoemd.

4.5 Opdrachtinstructies

De volgende opdrachten gaan over protocollen en worden gedaan in groepjes. Ieder groepslid is een van de personages Alice, Bob, Eve en Trent. Als je met meer dan 4 personen bent vervullen gewoon twee groepsleden samen de rol van een personage. Ieder personage heeft een paar open hangsloten en één bijbehorende sleutel. De sleutel is strikt persoonlijk: van elke sleutel is maar één exemplaar en de eigenaar van de sleutel zorgt dat niemand anders deze krijgt. Van de hangsloten die bij die sleutel horen zijn er meer exemplaren – zoveel als je maar wilt – en meerdere personages kunnen er daar een van hebben.[1]

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. 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. Verder 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

[1] Op `http://module-cybersecurity.cs.ru.nl` wordt meer informatie gegeven over materialen om deze opdrachten met echte sloten en sleutels na te spelen.

door in een open kistje zonder slot. De kistjes zijn te vergelijken met de IP pakketten op het internet, de kleine pakketjes informaties die computers op internet met elkaar uitwisselen om met elkaar te communiceren. (Het kistje is te vergelijken met een zogenaamd IP packet, een pakketje informatie dat verzonden wordt met het Internet Protocol.)

Een bericht hoeft niet per se een stukje geschreven tekst op een blaadje te zijn, het mag bijvoorbeeld ook een hangslot zijn.

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. De mogelijkheden voor Eve om de communicatie onmogelijk te maken komen overeen met een DoS (Denial-of-Service) aanval door Eve.

Verder 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. Bovendien, het is voor Eve veel interessanter om in plaats van de communicatie lomp te saboteren de communicatie op een subtiele manier aan te passen op zo'n manier dat de anderen niet in de gaten hebben dat Eve mogelijk berichten zit te veranderen.

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 voorbeeldopdracht met de oplossing erbij.

Voorbeeldopdracht: 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.

Oplossing:

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. Speel deze oplossing antwoord maar eens na om te zien hoe het werkt, en denk maar eens goed na of het klopt.

4.6 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 '→' 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:

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

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 als volgt:

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

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 afleiden 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:

$$A \rightarrow B : Slot_A$$

Met deze notatie ziet de oplossing van de voorbeeldopdracht 'E-mail versturen' er als volgt uit:

$$\begin{aligned} A &\rightarrow E : \{\text{Geheim bericht}\}_B \\ E &\rightarrow B : \{\text{Geheim bericht}\}_B \\ B &: \text{Geheim bericht} \end{aligned}$$

Opdracht 16 **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, in een doosje zonder slot.
3. Bob stuurt (via Eve) een van zijn geopende hangsloten naar Alice, weer in een doosje zonder slot.
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 17 **Berichten sturen via 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. (Bedenk dat er op internet miljarden mensen met miljoenen websites willen communiceren!) 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 van (a) 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 verstuurd heeft, dit leer je in het hoofdstuk 'Authenticatie'. Hoe kan Eve deze extra berichten sturen en waarom?

Opdracht 18 **Sleutels uitwisselen via 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:

$A \rightarrow T$: Hoi Trent, mag ik het slot van Bob? Groetjes, Anna
$T \rightarrow A$: $\{Slot_B\}_A$
A : $Slot_B$
$A \rightarrow B$: {Wil je met me uit, Bob? Liefs, Alice}$_B$
B : Wil je met me uit, Bob? Liefs, Alice

(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 doen om duidelijk te maken dat een bericht echt van hem afkomstig is, zodat Alice zeker kan weten dat de boodschap (het slot) dat ze ontvangt inderdaad van Trent komt en het slot is dat ze heeft gevraagd. Gebruik dat je ook meer dan één slot op een kistje kan dichtklikken, waardoor Alice het slot van Bob niet hoeft te hebben.

4.7 HTTPS

Als je naar een website gaat 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.

Om beveiligd met de bank te communiceren heeft je web-browser het hangslot van de bank nodig. De manier waarop je browser dat hangslot van de bank krijgt maakt gebruik van een vertrouwde partij zoals de Trent in de voorafgaande opdrachten. Het gaat in de trant van opdracht 4.6.

4.8 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 ook niet meer ervan uitgaan dat het vermelde slot van het bedrijf is. Een certificaat 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 dat dit certificaat echt is, dus dat het genoemde slot echt van Alice is, wordt gegeven doordat een bepaalde **autoriteit** zijn **digitale handtekening** op het certificaat zet. De Engelse term voor zo'n autoriteit is Certificate Authority, vaak afgekort tot CA. Een digitale handtekening is net zoals een gewone handtekening een bevestiging dat degene die de handtekening zet op een document, het eens is met dat document. Alleen is een digitale handtekening digitaal, dus met de computer gemaakt in plaats van handgeschreven. De autoriteit die de digitale handtekening zet, moet je dus vertrouwen om te kunnen concluderen dat het certificaat echt is. Als Trent het certificaat van Alice ondertekent zal Bob geloven dat het certificaat echt is, want Bob vertrouwt Trent. 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 19 **Bekijk certificaten in Firefox**

Ongemerkt misschien gebruikt jouw browser een heleboel certificaten. In deze opdracht ga je certificaten bekijken in Firefox. (Je kunt ook dit ook voor een andere browser doen, maar dan moet je zelf even uitvogelen hoe je in deze browser de certification kan zien.)

(a) Klik in Firefox bij 'Extra' op 'Opties', daarna op het tabblad 'Geavanceerd' en daarin op het tabblad 'Encryptie'. Klik vervolgens op 'Certificaten bekijken'. Zoek bij de tabbladen 'Servers' en 'Organisaties' naar bedrijven dat je kent en schrijf ze op.

(b) Bij 'Organisaties' staan de autoriteiten die jouw browser vertrouwt. Bij 'Servers' staan de certificaten die door een van de 'Organisaties' goedgekeurd zijn. Klik bij 'Servers' op een certificaat en dan op 'Weergeven...'. Onder het kopje 'Uitgegeven aan' staat over welke bedrijf dit certificaat gaat. Onder het kopje 'Uitgegeven door' staat welke autoriteit dit certificaat heeft ondertekend. Onder 'Geldigheid' staat vanaf welke tot welke datum het certificaat geldig is. Schrijf het bedrijf en de autoriteit op. Noteer ook wanneer het certificaat geldig is. Controleer vervolgens of de gevonden autoriteit ook te vinden is bij het tabblad 'Organisaties'.

(c) Na het klikken op 'Weergeven...' (in de Certificatenbeheerder) kun je op het tabblad 'Details' klikken. Als je klikt op 'Publieke sleutel van certificaathouder' (even scrollen) krijg je onder 'Veldwaarde' 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-websites ken je? Ga naar zo'n https-website en klik op het slotje in de URL-balk. Klik vervolgens op 'Certificaten bekijken'. 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.

4.9 Gebruik van cryptografie voor authenticatie

Je wilt niet dat andere mensen erachter kunnen komen wat jouw wachtwoord is. De bolletjes of sterretjes 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 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 20 Autosleutels

We willen op een veilige manier een autodeur openen 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 en opent de deuren.

$$AS \rightarrow A : IdNr$$
$$A : IdNr \text{ en } A \text{ opent de deur als het nummer klopt}$$

Is dit veilig?

(b) Nu versleutelen we het IdNr:

$$AS \rightarrow A : K\{IdNr\}$$
$$A : N + 1 \text{ en } A \text{ opent de deur als het nummer klopt}$$

Is dit veilig?

(c) Met 'N' geven we 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 het antwoord de waarde is van het tellertje en gaan de autodeuren 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, want elk cijfer wordt naar iets onvoorspelbaars vercijferd.

$$AS \rightarrow A : K\{N+1\}$$
$$A : N+1 \text{ en } A \text{ opent de deur als het nummer klopt}$$

Is dit veilig?

(d) Nu houdt alleen de auto het tellertje 'N' bij. De autosleutel hoeft niks te onthouden. Bij de laatste stap controleert de auto dat het antwoord van de sleutel klopt – d.w.z. dat het nummer is dat de auto stuurde plus – voor het de autodeuren opent.

$$AS \rightarrow A : \text{Open}$$
$$A \rightarrow AS : K\{N\}$$
$$AS : N$$
$$AS \rightarrow A : K\{N+1\}$$
$$A : N+1 \text{ en } A \text{ opent de deur als het nummer inderdaad } N+1 \text{ is}$$

Opdracht 21 **Wachtwoord uitwisselen**

(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. Ze willen dit wachtwoord natuurlijk nooit onversleuteld versturen. We gaan uit van een beginsituatie waarin Bob en Eve allebei het publieke slot van Alice hebben.

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

(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 bevestigd zijn met $\{\text{Bericht}\}_{A,B}$. Bob en Alice hebben elkaars publieke sloten niet nodig.

4.10 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 dat als Trent zijn slot aan hem geeft dat 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.

5 Digitale gevaren

Op het internet lopen we allerlei gevaren. Het bekendste voorbeeld is natuurlijk dat een computer die aan internet hangt, of een computerprogramma dat draait op een computer die aan internet hangt, **gehackt** kan worden: een aanvaller maakt dan gebruik van een beveiligingszwakheid om de werking van dat programma te verstoren, of, in het ergste geval, de computer waar het op draait helemaal onder zijn of haar controle te krijgen. Dit kan gebeuren met je laptop, tablet, of met je telefoon, maar ook met websites en met **servers**, de computers waar websites op draaien. Als een aanvaller de controle heeft gekregen over een computer, dan zullen aanvaller er vaak kwaadaardige software, oftewel **malware**, op zetten, om de computer voor hun doeleinden te misbruiken. Soms is het de aanvallers er enkel om te doen om data te stelen die op de computer staat, of om een website te **de-facen**. d.w.z. zelf de inhoud van de website aan te passen, als een internet-versie van graffiti.

Er zijn ook cybersecurity-problemen waar in principe helemaal geen computers voor gehackt hoeven te worden, zoals **spam**, **phishing**, en **DoS** aanvallen – al zullen criminelen vaak wel gehackte computers inzetten om deze aanvallen uit te voeren. Later meer over dit soort aanvallen.

De beveiligingszwakheden die gebruikt worden om systemen te hacken zijn vaak fouten in de software, ook wel **software bugs** genoemd. De meeste software is erg complex, en in de praktijk blijkt dat vrijwel alle software fouten bevat die een aanvaller kan misbruiken. Als zulke fouten ontdekt worden, dan kan de software – hopelijk snel – **gepatched** worden: Er wordt dan een verbeterde versie van de software gemaakt, waar de ontdekte fouten zijn verbeterd. Als gebruiker is het daarom van belang om alle software die je gebruikt zoveel mogelijk up-to-date te houden, om het risico dat je gehackt zo klein mogelijk te houden. Als zullen er vrijwel altijd nog andere fouten in zitten die nog niet ontdekt zijn...

Maar beveiligingszwakheden hoeven niet altijd in software te zitten: ze kunnen ook niet-technisch van aard zijn. Een bekend voorbeeld van zo'n niet-technisch probleem is domweg een slechtgekozen wachtwoord dat een aanvaller kan raden. Een ander voorbeeld is dat de aanvaller slachtoffers probeert te misleiden zodat ze uit vrije wil software van de aanvaller te installeren, bijvoorbeeld door zijn malware als **Trojan horse** in de Google PlayStore te zetten, of met **phishing** aanvallen en **scareware**.

In de rest van dit hoofdstuk gaan we in meer detail op sommige van deze bedreigingen in.

Opdracht 22 Zelf hacken

Om te begrijpen hoe het hacken van bijvoorbeeld een website in zijn werk gaat, en sowieso te begrijpen hoe websites werken, zijn er op internet allerlei voorbeeld-websites die je zelf kunt proberen te hacken. Onderaan op de webpagina bij deze module `http://module-cybersecurity.cs.ru.nl` vindt je links naar een paar van deze websites, waaronder ook een website die voor deze module is opgezet.

NB Het ongevraagd proberen te hacken van websites of andere computersystemen is strafbaar! In de Wet Computercriminaliteit wordt dit ***computervredebreuk*** *genoemd. Ga dus nooit ongevraagd proberen*

computersystemen binnen te dringen. Meer informatie over juridische aspecten rondom hacken kun je vinden in de blog van ICT-jurist Arnout Engelfried[1].

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 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 doordat zoveel mensen een mailtje binnenkrijgen. Behalve advertenties kan een spam-mailtje ook andere dingen bevatten, dit zal uitgelegd worden in 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-mailadressen verzameld worden. Vervolgens moet er een netwerk van computers ingezet worden om al die e-mails te kunnen verzenden en om onzichtbaar te maken waar de spam vandaan komt. Dit heet een **botnet**. Zo'n botnet bestaat vaak uit computers van mensen die een keer besmet zijn door malware (kwaadaardige software). Over malware volgt later informatie.[2]

Spam is niet alleen bij e-mail een probleem. Bij alle manieren om berichten te sturen kan spam een probleem worden. Ongewenste folders in je brievenbus is ook een vorm van 'spam', net als ongevraagde telefoontjes van mensen die je iets proberen te verkopen. In sommige landen in SMS spam een probleem. In mei 2015 waren de eerste incidenten met WhatsApp spam in Nederland. Natuurlijk zal het bedrijf achter WhatsApp – Facebook – er alles aan doen om spam op WhatsApp tegen te gaan, net zoals de telefoonbedrijven SMS spam zullen tegengaan.

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?

(d) Heb je wel eens ongevraagde berichten gekregen via andere kanalen dan e-mail die je als spam zou kunnen kwalificeren? Denk bijvoorbeeld aan Facebook Messenger, WhatsApp, Instagram, Skype of gewoon ouderwets bellen.

[1] `http://www.iusmentis.com/beveiliging/hacken/computercriminaliteit/computervredebreuk`
[2] Gebaseerd op notities van Leo Willems (Copyright leowillems.nl)

5.2 Phishing

Bij **phishing** doen criminelen zich voor als een persoon of instantie die je vertrouwt om zo gevoelige informatie te verkrijgen, bijvoorbeeld inloggegevens van internetbankieren. Die gegevens worden verkregen door het slachtoffer bijvoorbeeld naar een vervalste website te leiden. Meestal gaat phishing via e-mail, maar er kan ook gebruik worden gemaakt van andere communicatiekanalen.

Soms bijvoorbeeld wordt een slachtoffer opgebeld, waarbij een crimineel zich dan voordoet als ICT-medewerker, zoals in opdracht 4(b), of als iemand van de bank.

Soms is phishing gewoon ouderwetse oplichting, maar dan via moderne communicatiemiddelen. Maar soms wordt phishing gebruikt om mensen ertoe te verleiden om (kwaadaardige) software te installeren, zodat de phishing aanval enkel een springplank is naar een andere aanval. Over wat dit soort kwaadaardige software kan doen, zullen we in de volgende secties ingaan.

Zoals in de vorige sectie over spam al is opgemerkt, kan een e-mailtje gemakkelijk naar heel veel adressen gestuurd worden en zo veel mensen bereikt worden. Dit maakt het gebruik van e-mail aantrekkelijk voor een aanvaller. Hoe meer mensen, hoe groter de kans dat iemand het phishing-mailtje gelooft. Behalve voor advertenties is spam dus ook aantrekkelijk voor phishing.

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 uitziet. 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-mailberichten die je niet vertrouwt. 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 privégegevens 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 privégegevens van vrienden uitwisselt. Vermijdt voor het uitwisselen van dit soort gegevens, als het even kan, cloud-applicaties, mobiele applicaties en e-mailberichten.

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?

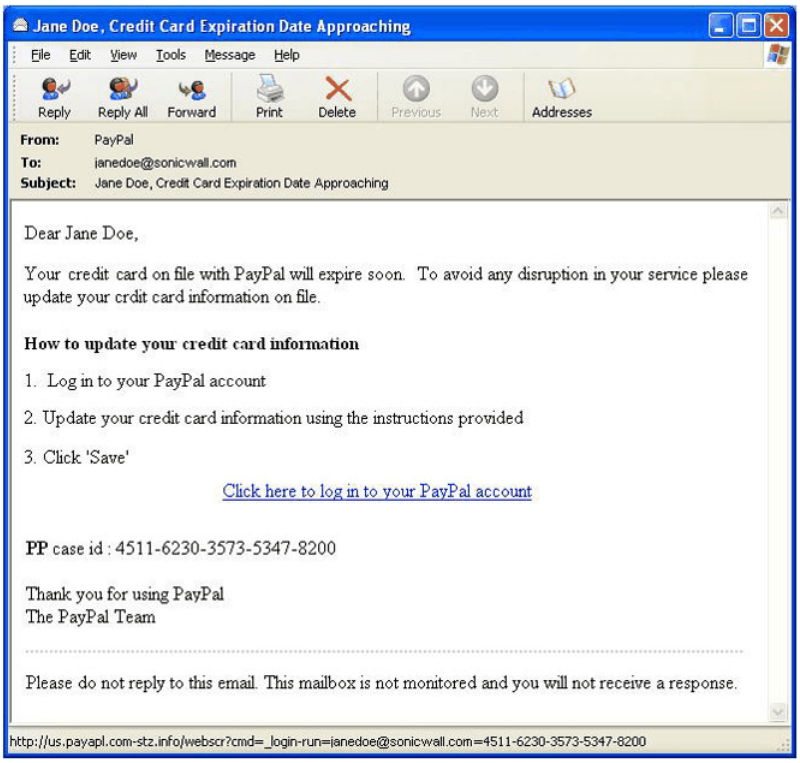
(b) Zo ja, wat waren de gevolgen?

[3] Gebaseerd op notities van Harald Vranken

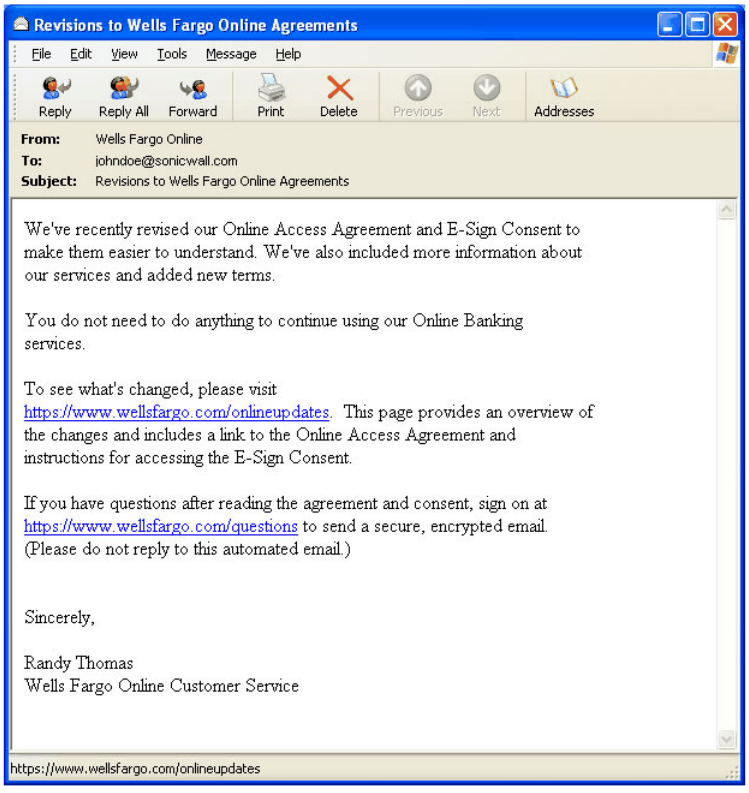
Opdracht 25 **Phishing-mails herkennen**

Bepaal voor elk van de volgende voorbeelden op de volgende bladzijde of er sprake is van phishing. Beschrijf welke aanwijzingen jouw standpunt ondersteunen.

(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 DoS-aanval

De afkorting **DoS** staat voor Denial of Service. DoS-aanvallen zorgen ervoor dat het systeem dat 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 DoS-aanval kan worden uitgevoerd door met een snelle computer of een botnet zó veel verbindingen op te zetten dat er geen nieuwe verbindingen gemaakt kunnen worden. Een enkele keer wordt er onbedoeld een DoS-aanval uitgevoerd op een website, bijvoorbeeld als heel veel mensen een concertkaartje willen kopen.

Een **DDoS** aanval – een *Distributed* Denial of Service aanval – is de DoS aanval die vanaf meerdere computers wordt uitgevoerd. In de praktijk zijn de meeste DoS aanvallen DDoS aanvallen.

Opdracht 26 **Recentste DoS-aanval**

(a) Wanneer was de recentste DoS-aanval?

(b) Welk systeem werd er aangevallen?

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

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

Figuur 5.1: Malware is binnengedrongen...

5.4 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, privacygevoelige gegevens verzamelen enz. De scareware en ransomware die hierboven genoemd zijn ook vormen van malware. Hieronder bespreken we drie belangrijkste vormen van malware: wormen, virussen en Trojan horses.

Wormen

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 computernetwerk is het internet. Een ander voorbeeld van een computernetwerk is dat computers van een bedrijf of school met elkaar verbonden zijn, waardoor gegevens gemakkelijk kunnen worden uitgewisseld. Bij scholen kan een leerling vaak inloggen op elke computer. Een worm kan zich verspreiden over een computernetwerk 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 verspreidt 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 zichzelf 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 een 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?

(c) Waarom was deze worm zo effectief?

Virussen

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 is het door iets onschuldigs als een PDF attachment openen, en zal hij dit zelf waarschijnlijk niet beseffen.

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.

Trojan horses

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 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 groep soldaten zich kon verbergen. De Grieken doen alsof ze wegvaren om geen argwaan te wekken bij de Trojanen. De Trojanen trekken vervolgens het paard de stad in omdat ze denken dat het paard een geschenk is van de godin Pallas Athena. '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, en
- goed getraind personeel.

Het bedrijf vroeg KPMG om binnen te dringen in het datacentrum, fysiek of digitaal. KPMG Amsterdam had namelijk een afdeling van mensen die gespecialiseerd waren in computerbeveiliging. 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 zijn ID-kaart toch niet te laten zien!

Figuur 5.2: Trojaanse Schimmel

Opdracht 29 **Social engineering**

Digitale gevaren maken vaak gebruik van het manipuleren of voor de gek houden van mensen om hen bepaalde acties uit te laten voeren of te zorgen dat ze gevoelige informatie afgeven. Deze manier van manipuleren noemen we ook wel **social engineering**. Bij welke onderwerpen en voorbeelden uit dit hoofdstuk wordt gebruik gemaakt van social engineering? Beargumenteer je antwoord.

Scareware en Ransomware

Scareware is een vorm van malware die probeert om de computergebruiker bang te maken, waardoor die eerder geneigd is een boete te betalen, gegevens af te staan, andere kwaadaardige software te installeren of een combinatie daarvan. Scareware kan als malware binnenkomen, of als popup op een website getoond worden. Zo'n pop-up kan dan proberen om de gebruiker software te laten installeren, zoals bijvoorbeeld de pop-up in figuur 5.3.

Figuur 5.3: Scareware die probeert om slachtoffers software te laten installeren.

Scareware kan ook proberen de computer te vergrendelen, zoals de scareware in figuur 5.4. Dit kan niet met een simpele pop-up op een webpagina: hiervoor moet de crimineel echt kwaadaardige software op je computer installeren. Men spreekt hier ookwel van **ransomware**, omdat je computer feitelijk gegijzeld wordt.

Figuur 5.4: Scareware die je computer vergrendelt, en zogenaamd van de politie is.

Omdat de vergrendeling van je computer mogelijk te omzeilen is, maken succesvollere – NB. succesvol voor de criminelen! – varianten van ransomware tegenwoordig gebruik van versleuteling. De ransomware versleutelt dan alle bestanden op je computer versleuteld. Om de bestanden weer terug te krijgen moet je geld betalen aan de criminelen: je krijgt dan de cryptografische sleutel waarmee alle bestanden weer te ontsleutelen zijn.

Ransomware is een zeer lucratief business model voor criminelen. Als een crimineel een manier heeft om zijn software op jouw computer te krijgen, dan is ransomware waarschijnlijk een van de beste manieren om hier geld mee te verdienen. Het versleutelen van de bestanden gebeurd gewoon op jouw computer zelf, dus dit kost de crimineel geen rekenkracht. De verdere aanval, inclusief het ontvangen van het geld – meestal in de vorm van bitcoins – kan volledig geautomatiseerd worden. Van Cryptowall

(zie figuur 5.5), de meest succesvolle ransomware variant uit 2015, wordt geschat dat er meer dan 300 millioen euro mee is buit gemaakt.

Je zou het misschien niet verwachten, maar in de praktijk blijkt dat veel vormen van ransomware inderdaad netjes je bestanden ontsleutelen als je betaalt. Dit doen de criminelen niet uit nobele motieven, maar gewoon om uiteindelijk zo veel mogelijk winst te maken. Als je namelijk van andere slachtoffers hoort dat je je bestanden niet terugkrijgt als je betaalt, dan zul je als slachtoffer minder snel geneigd zijn om toch maar te betalen. Het is voor de criminelen dus belangrijk dat hun ransomware een 'goede reputatie' heeft, in de zin dat je ook netjes je bestanden terugkrijgt als je betaalt.

Ransomware ontstreept het belang van goede back-ups maken! Regelmatig backups maken is verreweg de belangrijkste beveiligingsmaatregelen die je kan nemen, niet alleen voor een bedrijf, maar ook voor een privé-persoon.

Figuur 5.5: Screenshot van CryptoWall, een van de succesvolle variant van ransomware

Opdracht 30 **Malware schendt securitydoelen**

Leg uit welke securitydoelen geschonden worden door:

(a) phishing.

(b) een worm die zich alleen maar verspreidt.

(c) een virus dat zich alleen maar verspreidt.

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

(e) malware die bestanden verwijdert.

(f) malware die bestanden vercijfert.

5.5 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. Maak goede back-ups! Dit is verreweg de belangrijkste beveilingsmaatregel om te zorgen dat je bestanden niet kwijtraakt, mocht je een keer het slachtoffer worden van malware.
2. Houd software die je gebruikt – in elk geval je besturingssysteem, antivirussoftware en browser – zo goed mogelijk up-to-date. Het makkelijkste en beste gaat dit door software automatisch te laten updaten.
3. 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.
4. Gebruik een firewall. Windows en MacOSX bieden die al aan bij het besturingssysteem.
5. Maak gebruik van aparte gebruikersprofielen/accounts. Niet alle malware kan bij andere gebruikersprofielen naar binnen komen.
6. Download software alleen bij de fabrikant.
7. Installeer geen plugins of add-ons van onbekenden.

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

6 Privacy

6.1 Anonimiteit

In het hoofdstuk 'Inleiding cybersecurity' is al aan bod gekomen dat authenticatie anders werkt in de fysieke wereld (het dagelijks leven) dan 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 nickname en verder geen informatie over jezelf verstrekt, kun je denken dat je anoniem bent. De bekende cartoon van Pieter Steiner uit 1993 illustreert dat men in die begindagen van het internet dacht dat dit inderdaad zo was.

Peter Steiner's cartoon, oorspronkelijk verschenen in 1993 in *The New Yorker*

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.

Toch niet zo anoniem?

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. Je telefoonmaatschappij kan gegevens verzamelen over je bel- en sms-gedrag. 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, kan 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 512 tekens 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 jouzelf 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 advertenties of like-buttons. Die andere websites, die getoond worden op de website 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.

Om je privacy te beschermen kun je de cookies die je browser heeft verzameld geregeld weggooien. Je kunt sommige browsers ook zo instellen dat ze alle cookies automatisch weggooien als je de sessie afsluit. Er zijn ook browser-plugins die dit automatisch cookies weggooien, of gewoon helemaal nooit opslaan. Maar websites proberen altijd weer nieuwe truuks om je toch te kunnen volgen online! Een manier om dat te doen is met zogenaamde Flash cookies, die ook wel 'Local shared objects' heten. Net als cookies zijn dit zijn kleine bestandjes die op je computer worden opgeslagen, in dit geval door de Flash player die bij de meeste browser als plugin draait voor het tonen van Flash filmpjes of animaties.

Opdracht 32 **Cookies verwijderen in Firefox**

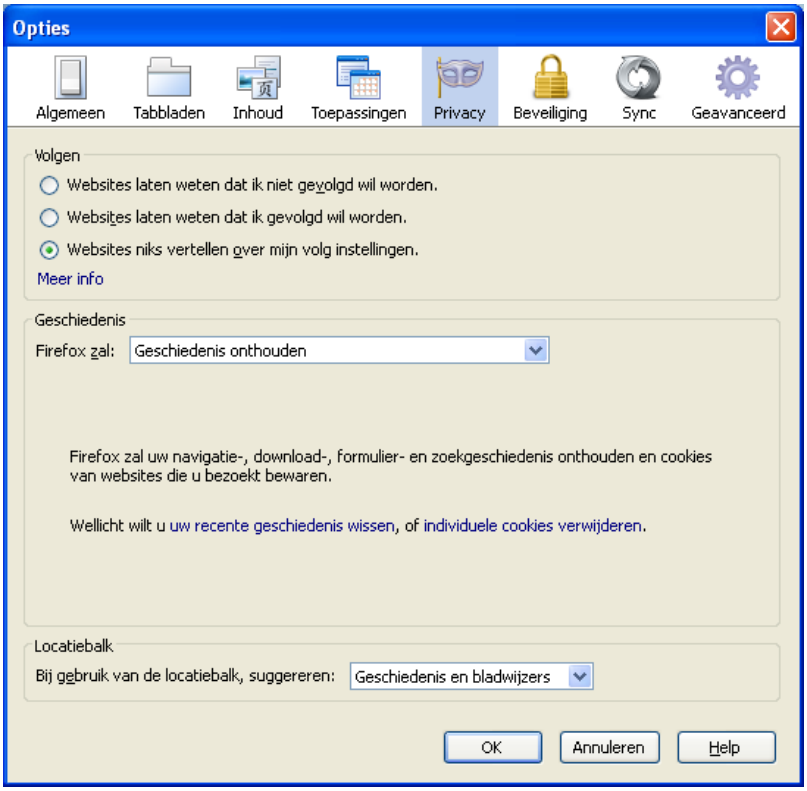
(a) Klik in het 'Extra'-menu op 'Opties'. Klik vervolgens op het tabblad 'Privacy'. Bovenaan kun je kiezen of je wilt dat Firefox aan websites laat weten of je gevolgd wilt worden (met cookies), of

dat je websites niks wilt 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 cookiebestand dat 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 afkomstig 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 6.1: Privacyinstellingen van Firefox

Figuur 6.2: Lijst met cookies

Opdracht 33 **De cookies die je krijgt terwijl je surft**

(a) Lightbeam 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 Lightbeam 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 hopelijk te vertrouwen en kun je op 'Installeren' klikken.

(b) Er verschijnt nu een Lightbeam ikoon in de top van het browser scherms. Als je hierop klink krijg je een nieuw tabblad, waarop je kan zien op welke websites je door wie allemaal gevolgd wordt.

(c) Ga nu (in een andere tab) naar een paar websites die je geregeld bezoekt. In de Lightbeam-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?

Opdracht 34 **Meer (anti)cookie plug-ins**

De Lightbeam addon probeert je een inzicht te geven in hoe je op verschillende websites gevolgd wordt. Er zijn ook plugins die proberen om cookies, en andere manieren om je te volgen, tegen te houden. Voorbeeld zijn de Privacy Badger en Ghostery, maar er zijn ook anderen.

Installeer de Ghostery plugin in Firefox, en configureer deze zo dat alle trackers en cookies geblokkeerd worden. Ghostery kan wel laten zien wie je allemaal probeert te volgen op een website (in de zogenaamde 'alert bubble' rechtsonder in je browser.

Probeer nu een website te vinden met de meeste andere partijen die je proberen te volgen. Websites met veel advertenties zijn een goede plek om uit te proberen. Lukt het je een webpagina te vinden met 10 andere partijen die je erop volgen.

6.4 Sociale media

Sociale media zijn er in allerlei soorten en maten: 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? Maak vrienden duidelijk welke gegevens ze wel en niet over jou online mogen zetten. Als sociale media privacyinstellingen aanbieden, gebruik deze dan, maar bedenk dat (de bedrijven achter) 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 6.3: Sociale media

Opdracht 35 Sociale media

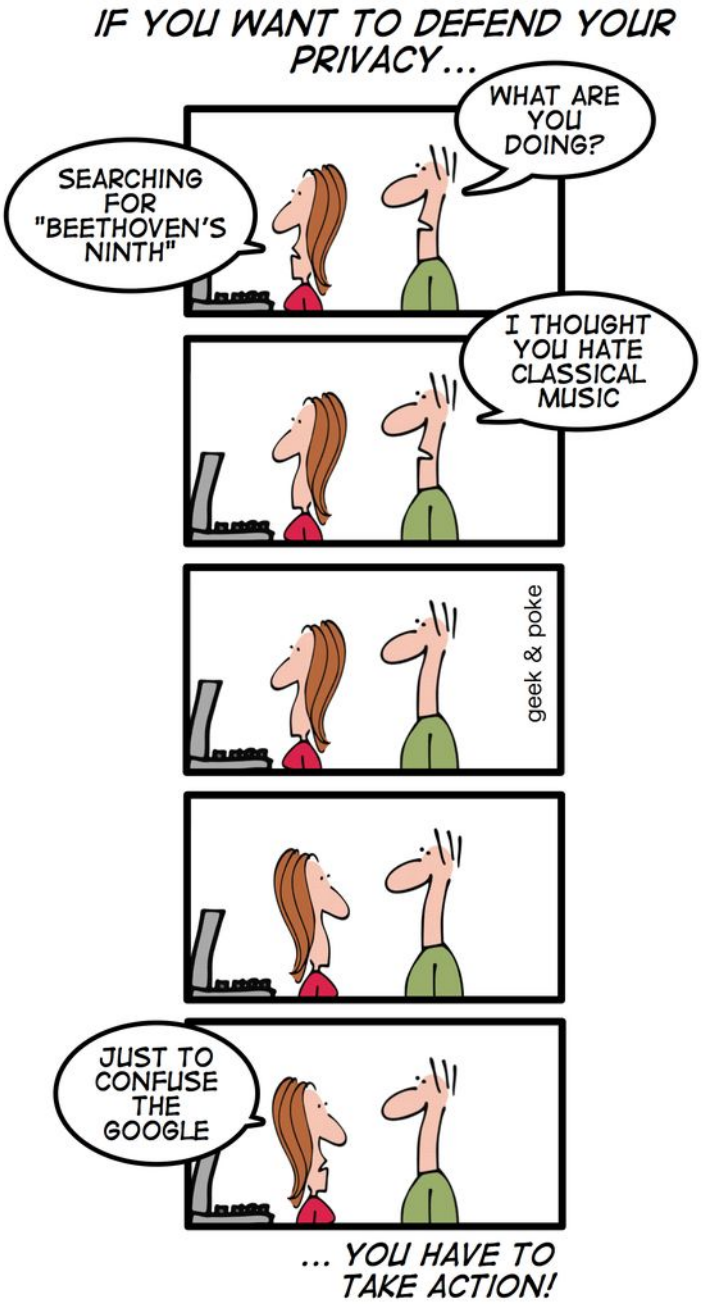
(a) Noem van elk van de genoemde soorten van sociale media een voorbeeld.

(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 (de bedrijven achter) sociale media veel over je weten? Beargumenteer je antwoord.



[Bron: Oliver Widder, `http://geek-and-poke.com`]