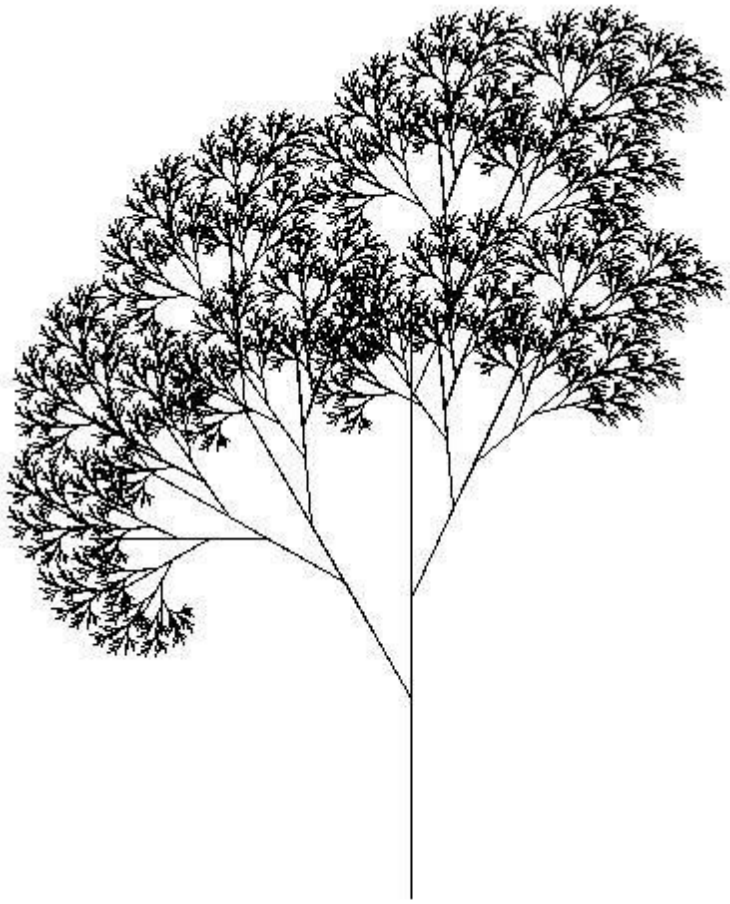


Informatica 12

remie.woudt@gmail.com

Voorblad:
Boom getekend met de programmeertaal LOGO, gebruik makend van recursie.

12 Cybercrime

12.1 Inleiding

En ineens is je rekening leeg

- Cybercriminelen gaan steeds slimmer te werk
- Laatste trend is 'man in the browser-attack'
- "Zorg dat je computer schoon blijft"

▶ Computercriminelen worden steeds slimmer om consumenten om de tuin te leiden.

Een schone computer

- Zorg voor een goede antivirussoftware. Deze is voor nop verkrijgbaar bij AVG (http://free.avg.com) en Avast (http://www.avast.com)
- Zet je firewall aan en zorg dat er niet onnodig poorten openstaan.
- Hou je Windowssoftware en programma's als Adobe up-to-date.

Zonder dat je het doorhebt is je bankrekening leeg of blijk je duizenden mailtjes te hebben verzonden, waardoor je internetaccount wordt afgesloten. In Nederland worden iedere week tientallen computergebruikers slachtoffer van zogenaamde botnetwerken. Daarbij worden computers gebruikt als onderdeel van een crimineel internetnetwerk.

De laatste trend is de zogenaamde 'man in the browser-attack'. "Daarbij nestelt een programmaatje zich in je browser en speelt inloggegevens van je bank door aan criminelen", legt Alex de Joode van hostingprovider Leaseweb uit. "Daarnaast zijn er programmaatjes die je computer gebruiken om spam te versturen. Word je ineens afgesloten door je provider zonder dat je dat zelf weet." Volgens De Joode is het belangrijk om te zorgen dat je computer schoon blijft (kader).

Onlangs werd een groot botnetwerk opgerold dat actief was via een van de dertigduizend servers van Leaseweb. "Wij kregen een melding en wilden tot sluiting overgaan, maar op verzoek van de KLPD hebben we dat niet gedaan. Zij gingen op zoek en dat leidde tot de arrestatie van een kopstuk in Armenië." JOB HALKES

Afbeelding 1: Artikel uit de Metro van 10 november 2010

Elke keer dat er een nieuwe (technische) ontwikkeling plaatsvindt, zijn er mensen die er misbruik van maken. Soms om er (grof) geld aan te verdienen maar soms ook gewoon voor de lol. En zo gebeurde dit ook bij het internet. Toen het web nog klein was leverde dit relatief weinig schade op. Maar nu het web steeds groter wordt, in 2010 maakte ruim 2 biljoen mensen gebruik van internet, wordt de schade ook steeds groter. En met een grote winkans en een kleine pakkans is het er voor internetcriminelen goed vertoeven.

Het doel van deze module is de gevaren van internet inzichtelijk maken; hoe doen ze het en hoe kun je dit gemakkelijk voorkomen. Ook zullen we de wet en de groeiende invloed van Social Media behandelen.
Bijna alle vormen van criminaliteit hebben baat bij het internet. Maar daarnaast gaan we ook in op criminaliteit die niet online plaatsvindt maar wel met behulp van computers.

12.2 Computercriminaliteit

Computercriminaliteit is geen nieuw fenomeen maar met het toenemen van het aantal computers lijkt deze vorm van criminaliteit zich enorm uit te breiden. De criminaliteit wordt niet alleen steeds heviger en schadelijker, ook worden steeds nieuwe vormen van computercriminaliteit uitgedacht en toegepast.

Als je het artikel van afbeelding 1 leest dan lijkt de situatie niet erg hoopgevend. Het valt niet mee om de criminelen buiten de deur te houden. Je vraagt je zelfs af of het nog wel verstandig is om je eigen PC aan te zetten. Per slot van rekening vindt niemand het leuk om plotseling een lege bankrekening te hebben.

In dit hoofdstuk gaan we in op de vele vormen van computercriminaliteit of cybercrime. Hier onder verstaan we criminaliteit op internet, via e-mail en ook zogeheten RFID-chips. Je komt hier meer te weten over de gevaren die je tegenkomt op het moment dat je je computer op het internet aansluit. Via het internet kun je bijvoorbeeld heel handig dingen snel opzoeken en spelletjes spelen en via e-mail, Skype en de sociale netwerken als Facebook, Instagram enz. kun je gemakkelijk contact houden met vrienden. Maar het internet is beslist niet ongevaarlijk. Denk bij gevaren bijvoorbeeld aan virussen en hackers, maar ook aan spam en phishing e-mails. Al deze onderwerpen zullen hier behandeld worden. Wat zijn de gevaren precies? Hoe werken ze? En ook hoe je je ertegen kunt wapenen door spamfilters en virusscanners te installeren.

Gelukkig is er ook nog de wet. In de wet staan een aantal artikelen over computercriminaliteit. Er staat natuurlijk in dat het niet mag, maar wat mag er dan precies niet?

12.2.1 Vormen van computercriminaliteit

Zoals in de inleiding al besproken is, is het internet een groeiend netwerk. In juni 2010 gebruikte ongeveer 1,9 biljoen mensen het internet, een groot gedeelte van deze mensen en de bedrijven en organisaties heeft weinig idee van beveiliging en heeft dit ook niet toegepast op hun eigen computers.

Enkele voorbeelden:

- *Rond de Kerst van 2006 was het percentage spam zo hoog opgelopen dat tot tweemaal toe de mailserver van een bekende Nederlandse provider het niet meer aan kon. Het e-mail verkeer kwam tot stilstand. Wereldwijd wordt de schade als gevolg van spam op 50 miljard dollar geraamd.*
- *Door politieke motieven gedreven hackers hebben in januari 2007 ingebroken in de computers van het Belgische leger. Vervolgens hebben ze de website voorzien van andere informatie. Bezoekers die vervolgens de website bezochten kwamen terecht op een andere website.*
- *Zowel de provider als het Belgische leger zijn professionele organisaties en toch blijken ze niet in staat om de criminelen buiten de deur te houden.*
- *Het skimmen van betaalpassen kostte de Nederlandse banken in 2009 zo'n 36 miljoen euro. Dit was het resultaat van zo'n 32.000 geskimde bankpassen. Dit is meer dan €1000 per bankpas met een eenmalige actie.*
- *Begin 2011 werd bekend dat de VS en Israël waarschijnlijk een worm hebben ontwikkeld die specifiek de systemen van (Iraanse) kerncentrales om zeep helpt. Ook worden de Russen ervan verdacht verschillende Estische overheidssites platgelegd te hebben als reactie op het verwijderen van een Russisch oorlogs-standbeeld. Hierop is een nieuw woord ontstaan: Cyberwarfare oftewel het oorlogsvoeren met behulp van virussen en wormen.*
- *In september van 2011 werd bekend dat het bedrijf DigiNotar een aantal foute certificaten heeft uitgegeven. Dit kon gebeuren doordat het bedrijf was gehackt door (vermoedelijk) Iraanse hackers. Hierop volgde een internationale onrust en werden alle veiligheidscertificaten van de (Rijks)overheid ongeldig verklaard.*

Opdracht 1

Op de website http://www.om.nl/onderwerpen/cybercrime/ vind je veel informatie. Onder het kopje Video's vind je twee filmpjes. Bekijk deze en vat ze in een paar zinnen samen.
Doe hetzelfde met deze filmpjes:
http://www.waarschuwingsdienst.nl/Risicos/Virussen+en+malware/Animatiefilm+over+virussen,+wormen+en+andere+gevaren+op+het+internet.html
http://www.youtube.com/watch?feature=player_detailpage&v=8m5GnLxzuO8
http://www.youtube.com/watch?feature=player_detailpage&v=3irXZ6IwUjE
http://www.youtube.com/watch?feature=player_detailpage&v=BWP6Mdnr7is
http://www.youtube.com/watch?feature=player_detailpage&v=uzASXrhbCXY
http://www.youtube.com/watch?feature=player_detailpage&v=RQBn_ZB65m4

Opdracht 2

Wat bedoelen ze met 'geldezels'?

Opdracht 3

Zoek uit hoeveel verschillende vormen van computercriminaliteit er zijn en hoe ze werken. Probeer zoveel mogelijk manieren te verzamelen.
TIP: de site van de waarschuwingsdienst (http://www.waarschuwingsdienst.nl/) en van het Nationaal Cyber Security Centrum (https://www.ncsc.nl/) kunnen hierbij erg handig zijn.

12.3 Kwaadaardige software

Allereerst kijken we naar voorbeelden van kwaadaardige software. Dit type software wordt ook wel malware (malicious software) genoemd. De software is kwaadaardig omdat ze probeert je computer over te nemen en processen uit te voeren die jij als gebruiker niet wilt. In het ergste geval kan je computer onbruikbaar worden. Het gaat hier om:

- Virussen
- Wormen
- Trojaanse paarden
- Botnets

12.3.1 Virussen

Een virus is een computerprogramma dat zich op je computer kan bevinden, vaak zonder dat jij daar weet van hebt. Alhoewel dit soms weinig kwaad kan, worden

computervirussen in het algemeen als schadelijk beschouwd. In ieder geval nemen ze schijfruimte en computertijd in beslag. In ernstige gevallen kunnen ze in de computer meer schade aanrichten. Bijvoorbeeld het verwijderen van belangrijke bestanden of het verspreiden van gevoelige informatie.

Virussen zijn gemaakt om zichzelf te dupliceren en te verspreiden. Op die manier besmetten ze zoveel mogelijk computers. Net als organische virussen (het griepvirus bijvoorbeeld) kunnen computervirussen niet apart bestaan. Het zijn altijd stukjes code die aan een ander programma vastgeplakt zitten.

Er bestaan verschillende soorten virussen. De belangrijkste typen zijn:

- **Bestandsvirus**: Een bestandsvirus hecht zichzelf aan een programmabestand. Programmabestanden zijn de bestanden die je uit kunt voeren; je kunt ze herkennen aan de extensies .EXE of .COM (onder extensie verstaan we de letters achter de punt in een bestandsnaam). Zodra een besmet programmabestand geopend wordt, wordt het virus actief.
- **Macrovirus**: Macrovirussen komen met name voor in Word- of Excel-documenten. Ze worden actief als het document gestart wordt. Macrovirussen komen bijna niet meer voor, de laatste grote uitbraak was in 1999.
- **Bootsectorvirus**: Bootsectorvirussen richten schade aan in de bestanden die nodig zijn om een computer op te starten. Een bootsectorvirus kan er voor zorgen dat een computer niet meer kan worden opgestart.
- **Polymorf virus**: Een polymorf virus verandert zich uiterlijk elke keer als het zich verspreidt.
- **Tijdbom virussen**: Tijdbom virussen zijn geprogrammeerd om op een bepaalde datum of tijd in actie te komen. Daarvóór doen ze niets.
- **Mobielvirus**: Een mobielvirus richt zich niet op computers, maar op mobiele telefoons of PDA's. Het virus kan zich verplaatsen van de ene mobiele telefoon naar de andere.

Opdracht 4

1. Wat is de meest gebruikelijke manier om een virus binnen te krijgen?
2. Noem 3 verschillende, recente virussen die veel schade veroorzaakten.
3. Is het schrijven van een virus strafbaar? En het verspreiden?
4. Wat is de beste manier om een virus te verspreiden?

12.3.2 Wormen

Een worm wordt door de meeste mensen gezien als iets dat hetzelfde is als een virus. Technisch gezien is dat niet juist. Een worm kan zich namelijk, in tegenstelling tot een virus, zelfstandig verspreiden. Ook hoeft de gebruiker bij een worm helemaal

niks te openen of te bekijken. De code voert zichzelf uit zonder dat je er omkijken naar hebt.
Dit zorgt ervoor dat een worm zich razendsnel kan verspreiden over de verschillende computers, en in een kort tijd erg veel computers kan besmetten. Hierdoor zijn wormen meestal een stuk schadelijker dan “gewone” virussen.

De eerste worm op het internet werd gemaakt door Robert Morris. De worm heette daarom ook de Morris Worm. In 2004 verspreidde zich de W32/Amus-A worm via e-mail. Als een gebruiker het mee gestuurde bestand opende, dan werd er een boodschap voorgelezen. Deze pratende worm maakte gebruik van de Microsoft speech engine in Windows.

In juni 2010 kwam er weer een nieuwe worm in het nieuws, stuxnet. Deze leek zich specifiek op Iraanse kerncentrales te richten. Opdracht 5.4 gaat hierover.

Opdracht 5

1. In welk jaar werd de eerste worm gemaakt en verspreid?
2. Waarom verspreidt een worm zich sneller dan een virus?
3. Bestaan er ook goedaardige wormen?
4. Zoek op internet naar informatie over de stuxnet-worm, wat doet deze worm precies?
5. Wat maakt deze worm zo speciaal, en wordt deze in de media zo breed behandeld?

12.3.3 Trojaanse paarden

Een Trojaans paard is een programma dat nuttig lijkt maar heel vervelende eigenschappen heeft. Je downloadt het programma omdat je denkt dat het nuttig is, maar nadat je het programma gestart hebt blijkt vaak dat het programma de beveiliging op je PC lekt heeft geprikt.

Een Trojaans paard vermenigvuldigt zichzelf niet zoals wormen en virussen dit doen, maar zorgt ervoor dat gebruikers zelf de code binnenhalen. Het programma komt meestal in de vorm van een handig hulpprogramma, leuke screensaver of als zogenaamde upgrade. Een voorbeeld hiervan is een Trojaans paard dat zich voordeed als een gratis programma tegen de Blasterworm. Maar wie het programmaatje installeerde zette zijn computer open voor hackers.

De naam Trojaans paard heeft te maken met een verhaal over de Trojaanse Oorlog (rond 1180 voor Christus). Al tien jaar vochten de Grieken tegen de Trojanen. Maar het lukte de Grieken maar niet om de stad Troje in te nemen. Daarom bedacht de Griek Odysseus een list. De Grieken bouwden een reusachtig houten paard. In de

buik van het paard verstopten zich soldaten. Dit paard werd ’s avonds voor de poort van Troje achtergelaten. De Grieken verzonnen een list zodat de Trojanen dachten dat het paard van Pallas Athena kwam en de stad zou beschermen. De Trojanen trapten in de list en haalden het paard met veel moeite binnen in de stad. De Trojanen dachten dat ze gewonnen hadden en vierden de hele avond feest om de overwinning te vieren. ’s Nachts toen alle Trojanen, moe en dronken van het feesten, sliepen, verlieten de Grieken het paard en openden de poorten zodat ook de Grieken die nog buiten waren naar binnen konden. De Trojanen waren te moe en te dronken om de stad nu nog te verdedigen.
De Grieken staken alles in brand en binnen korte tijd was er niets meer van Troje over.

Opdracht 6

1. Wat zijn de overeenkomsten tussen virussen, wormen en Trojaanse paarden?
2. Wat zijn de verschillen tussen virussen, wormen en Trojaanse paarden?

12.3.4 Botnets

Een bot is een programma dat zelfstandig geautomatiseerde taken kan uitvoeren. Zo worden bots vaak gebruikt om zaken te doen die bijna onmogelijk zijn voor mensen. Het woord bot komt van robot. Voorbeelden van bots zijn:

- ***Zoekmachine-bots***: Zoekmachines zoals Google gebruiken een bot om alle websites in kaart te brengen
- ***Shopping-bots***: Een shopping bot zoekt automatisch de laagste prijzen op internet voor een bepaald product
- ***Spam-bot***: Een spam bot is een nogal vervelend soort bot. Zo bestaat er een spambot die zich automatisch inschrijft op fora en vervolgens alleen maar reclame-berichten post.

Een bot kan dus heel onschuldig zijn maar ook heel vervelend. Een computer die besmet is met een bot wordt ook wel een zombie genoemd. Een botnet is een netwerk van een groot aantal willoze zombies die allemaal besmet zijn met dezelfde bot. Vanuit één centraal punt (de Bot Herder) kan een kwaadwillend persoon alle zombies in het netwerk opdracht geven dezelfde taak uit te voeren, bijvoorbeeld een zogenaamde Distributed Denial of Service (DDoS) aanval. Hierbij gaan alle computers in het netwerk op hetzelfde moment een bepaalde webpagina opvragen en ze doen dit meerdere malen per seconde. Hierdoor wordt er zoveel verkeer op de webserver van de internetpagina gegenereerd dat deze de vele verzoeken niet meer aan kan en de site voor goedwillenden ook niet meer beschikbaar is.
Een bekend voorbeeld is de site van WikiLeaks in 2010. Hun site werd na het publiceren van honderden Amerikaanse ambtsberichten aangevallen waardoor deze

een lange tijd uit de lucht was en zelfs andere pagina's op dezelfde server niet meer beschikbaar waren.
Een ander voorbeeld hiervan is de mislukte chatsessie met Willem-Alexander en Maxima in 2002. Een groep van acht zeer ervaren hackers voerde een massale aanval uit op de computers van KPN. In enkele seconden tijd bezweken deze onder de grote hoeveelheid data die via internet aankwam. Hierdoor kon de chatsessie niet meer doorgaan.

Opdracht 7

1. Hoe krijg je een bot op je computer?
2. Zoek nog eens een voorbeeld van een DdoS aanval.

12.4 Wat kun je er aan doen?

In het vorige deel heb je gezien wat voor kwaadaardige software er allemaal bestaat. Als je de teksten zo leest, kun je al snel het idee hebben dat het internet een erg gevaarlijke en ongure plek is. Maar gelukkig kun je je als internetgebruiker goed beschermen tegen al die gevaren.

Hoe kun je dan virussen bestrijden?

1. De belangrijkste maatregel is het installeren van een virusscanner
2. Een tweede maatregel om virussen te bestrijden is om voorzichtig te zijn met het openen van bestanden die je van anderen hebt gekregen. Open nooit bijlagen van e-mails van personen die je niet kent.
3. Een derde maatregel is het goed updaten van alle software. Virusmakers maken gebruik van fouten in software. Softwaremakers lossen deze fouten weer op door middel van patches. Het is belangrijk om als gebruiker van deze software op tijd deze patches te installeren.

12.4.1 Anti-virussoftware

Om computervirussen te kunnen tegengaan, is er anti-virussoftware beschikbaar. Deze software kan virussen opsporen en vaak ook verwijderen. Anti-virussoftware maakt gebruik van verschillende technieken om te controleren of ergens een virus in zit.

12.4.1.1 De scanners

Virusscanners maken gebruik van virusdefinities waarin voor elk bekend virus de vingerafdruk oftewel de fingerprint wordt vastgelegd. De fingerprint van een virus is een stukje code van het virus dat altijd hetzelfde is. Aan de hand van de fingerprint kan een scanner een virus dan herkennen. Het grootste nadeel van deze techniek is dat scanners alleen virussen kunnen ontdekken waarvan ze de fingerprint kennen. Voor ieder nieuw virus geldt dat er eerst ergens een slachtoffer moet vallen voordat de makers van de scanner een bruikbare fingerprint kunnen vaststellen. En die fingerprint moet dan aan de scanners worden doorgegeven. Daarom is het belangrijk om je virusscanner vaak te updaten, zodat je altijd de nieuwste fingerprints hebt.

Opdracht 8

1. Wat is een nadeel van de scanner methode?
2. Wat is een voordeel van de scanner methode?
3. Kan deze methode ook polymorfe virussen herkennen?
4. Zoek op de site van Symantec naar het laatst ontdekte virus http://us.norton.com/security_response/threatexplorer/index.jsp

12.4.1.2 De checksummers

Checksummers maken gebruik van de checksums van alle bestanden op de computer. Een checksum is een controlegetal dat uitgerekend wordt aan de hand van de inhoud van een bestand. Wanneer een programma wordt besmet, verandert het bestand en daarmee ook het controlegetal. De virusscanner controleert dus steeds of de checksum van elk bestand nog hetzelfde is als de checksum die in de lijst staat.
Een voorbeeld van een checksum is de MD5-functie. Dit is een functie die elke string omzet in een “getal” van 32 tekens. Aan de hand hiervan kan dus elk bestand een afzonderlijk getal krijgen. Een bijkomend voordeel is dat vanuit de checksum (of hash) niet achterhaald kan worden wat de oorspronkelijke string was. Dit maakt de MD5-methode een veelgebruikte methode voor wachtwoordopslag (later meer hierover).

Opdracht 9

1. Wat is een nadeel van de checksum-methode?
2. Wat is een voordeel van de checksum-methode?
3. Kan deze methode ook polymorfe virussen herkennen?
4. Maak een MD5-hash van je naam en maak erna nog een met een spelfout erin. Wat zijn de verschillen? Je kunt dat doen op o.a.:
5. http://www.netadvies.nl/tools/MD5-Hash-Generator.php

12.4.1.3 De heuristische scanners

Een heuristische scanner controleert bestanden op eigenschappen die typisch zijn voor virussen. Voorbeelden van zulke eigenschappen zijn bijvoorbeeld: code om een datum te controleren of code die het adresboek van je e-mailprogramma raadpleegt.

Zo zijn er nog een aantal acties die kenmerkend voor virussen zijn. Op het moment dat deze opgemerkt worden zal deze scanner ingrijpen. Dit heeft als voordeel dat nieuwe virussen meteen ontdekt worden, maar als nadeel dat veilige programma's ook tegengehouden worden.

Opdracht 10

1. Wat is een nadeel van de heuristische methode?
2. Wat is een voordeel van de heuristische methode?
3. Kan deze methode ook polymorfe virussen herkennen?

Een goede virusscanner maakt tegelijkertijd gebruik van alle drie de technieken!

12.4.2 Patches

Niet alleen de virusscanner moet geüpdate worden. Ook makers van andere programma's brengen vaak patches uit. Een patch is een kleine wijziging in een programma om het programma te repareren of te verbeteren. Hierdoor worden ernstige beveiligingslekken in een programma gedicht. Het is aan te raden om patches altijd zo snel mogelijk te installeren.

12.5 Virtueel inbreken en afluisteren

In deze paragraaf gaat het over virtueel inbreken. Daarmee bedoelen we:

- Hacken
- Spyware
- Wardriving

12.5.1 Hacken

> *In deze paragraaf wordt regelmatig gesproken over hackers. Vrijwel altijd denken we dan aan mensen die in computers of netwerken inbreken. Ook als we het werkwoord hacken lezen denken we aan iemand die aan het inbreken is. Maar in Amerika is een hacker een uitzonderlijk goede programmeur. Iemand die naast het beheersen van de programmeertaal ook inlevingsvermogen heeft in de toekomstige gebruiker van het computersysteem. Voor veel programmeertalen zijn zogenaamde Hacker's*

guides geschreven. Boeken dus waarin de fijne kneepjes van die programmeertaal uit de doeken wordt gedaan. In Nederland kennen we geen specifieke vertaling voor de hier genoemde hackers. Voor wie meer wil weten, lees het boek “Hackers and painters” van Paul Graham.

Hackers (zoals we het woord in Nederland gebruiken) en crackers doen hetzelfde: inbreken in een andere computer. Maar toch is er een groot verschil tussen hacken en cracken. Een hacker is iemand die om idealistische redenen de beveiliging van systemen test op fouten en daar verbeteringen voor probeert te vinden. Een cracker is een kwaadwillend persoon, die zich bezig houdt met illegaal toegang verschaffen tot een andere computer.
Een hacker wordt ook wel een white-hat hacker genoemd en een cracker een black-hat hacker. Deze termen komen uit cowboyfilms waarin de "kwaden" zwarte hoeden droegen en de "goeden" witte hoeden.
Een white-hat hacker is geliefd in het bedrijfsleven. Bedrijven huren ze in om de beveiliging van hun systemen te testen. Zo hopen ze de black-hat hackers buiten de deur te houden.

Naast hackers en crackers is er ook nog de categorie scriptkiddies. Scriptkiddies zijn personen zonder kennis van programmeren die het leuk vinden om virussen te maken en te verspreiden. Het is mogelijk om van het internet software te downloaden waarmee je zonder enige kennis van zaken een virus kunt maken. Het blijkt dat veel virussen door scriptkiddies gemaakt zijn.

12.5.1.1 Exploits

Maar hoe werkt hacken dan? De meeste hackers, crackers en scriptkiddies maken gebruik van exploits. Een exploit is een kwetsbaarheid in de hardware of software. Een zero-day exploit is een net ontdekte kwetsbaarheid. Zero-day exploits zijn extra gevaarlijk omdat de makers van de software waarin de exploit zit vaak nog niet eens weten hoe ze de software moeten beveiligen.

12.5.1.2 Social engineering

Naast exploits gebruiken crackers vaak ook sociaal hacken oftewel social engineering. Dit is een techniek waarbij de hacker een inlognaam en wachtwoord probeert te achterhalen via een mens. Een methode is bijvoorbeeld om een bedrijf te bellen en de receptioniste te vertellen dat alle computers besmet zijn met een ernstig virus en dat je nu het wachtwoord nodig hebt om de informatie op de computers te kunnen redden. Als de secretaresse dan toehapt en het wachtwoord geeft, ben je als cracker binnen.

Opdracht 11

1. Waarom hacken mensen?

2. Was de schrijver van het Kournikova virus een hacker, cracker of scriptkiddie?
3. Wat zijn tigerteams?
4. Leet speak is de onofficiële taal van de hackers. Weet je wat hier staat : n00b I5 133t 5p34k v00r b39InNER

12.5.2 Spyware

Spyware is een samentrekking van de woorden spy en software en betekent spionagesoftware. Spyware is de verzamelnaam voor de volgende types software:

- **Trackingcookies**: Een cookie is een klein bestandje met informatie dat op je computer terecht komt na het bezoeken van een website. Vaak zijn cookies nuttig: ze onthouden bijvoorbeeld je instellingen of loginnaam voor een bepaalde site. Trackingcookies zijn minder onschuldig, ze volgen je surfgedrag (dus welke websites je bezoekt) en sturen dat door naar de site dat het trackingcookie heeft geplaatst. Zo is het voor bedrijven mogelijk om met trackingcookies je surfgedrag te volgen.
- **Reclame banners**: Een reclame banner is een pop-up venster met reclame. Naast de pop-up schermpjes bestaan er ook pop-under vensters. De verbergen zich onder de openstaande vensters. Je ziet het pop-under scherm dus pas later als je de openstaande vensters wegklikt. Reclame banners zijn niet gevaarlijk, maar kunnen wel irritant zijn.
- **Browser hijackers**: Browser hijackers zorgen ervoor dat bepaalde aspecten van de browser aangepast worden. Hierbij is te denken aan het aanpassen van startpagina's, zoekpagina's of favorieten zonder dat je dat zelf wilt.

Afbeelding 2: Een keylogger

- **Keyloggers**: Keyloggers zijn programma's die elke toets die jij op je toetsenbord intikt registreren. Hiermee kun je dus wachtwoorden of andere gevoelige informatie achterhalen. Er bestaan ook hardware keyloggers (zie afbeelding 2). Deze plaats je tussen je computer en je toetsenbord. De hardware keylogger kan niet gevonden worden door een virusscanner, de

softwareversie vaak wel.

Opdracht 12

Stel dat de school een cookie plaatst op je computer als je de schoolsite opent. Op deze manier kan de school kijken hoeveel je achter de computer zit. Wat vind je hiervan?

Opdracht 13

- Op welke manier komt spyware op je computer?
- Op welke manier kun je spyware bestrijden?
- Zoek op: Wat is snoopware?

12.5.3 Wardriving

Wardriving is rondrijden met een auto met de bedoeling draadloze netwerken te vinden. Een draadloos netwerk is een computernetwerk waarbij de aangesloten apparaten niet via kabels met elkaar communiceren maar via radiogolven. Het voordeel van een draadloos netwerk is dat je geen kabels hoeft te leggen en dat je op elke willekeurige plek in je huis kunt internetten.
Voor een draadloos netwerk heb je een basisstation nodig. Dit apparaat zorgt voor de verbinding. Meestal is dit basisstation een draadloze router. Als je een computer hebt die draadloze netwerken ondersteunt dan kun je contact maken met het basisstation en op die manier bijvoorbeeld gebruik maken van internet.
Het nadeel van een draadloos netwerk is dat radiogolven door muren en ramen gaan dus dat ook je buurman contact kan maken met jouw basisstation. De meeste draadloze netwerken maken zich bekend door continu hun naam te versturen. Deze naam noemen we het SSID. SSID staat voor Service Set Identifier. Wardrivers zijn in hun auto continu op zoek naar SSID's.
Om te voorkomen dat je buurman of wardrivers gebruik kunnen maken van je draadloze netwerk is het belangrijk dat je je draadloze netwerk goed beveiligt.
Naast wardriving zijn er ook mensen die aan warwalking (wandelen), warcycling (fietsen) en warstorming (rondvliegen) doen. En er zijn ook mensen die niet op zoek zijn naar draadloze internetverbindingen maar naar bijvoorbeeld telefoons met een bluetooth verbinding.

Als je als wardriver een netwerk hebt gevonden, wil je dat aan andere wardrivers laten weten. Dat kan op twee manieren:

- Warchalking is het met krijt aangeven in publieke ruimtes of er een draadloos netwerk in de buurt is. Ook geven ze
  aan of het goed of slecht beveiligd is.
  De twee belangrijke tekens die ze

gebruiken zie je in afbeelding 3. Het onderste teken geeft een beveiligd netwerk aan. Het bovenste teken een onbeveiligd netwerk.

- De andere manier om aan te geven waar onbeveiligde netwerken zijn is natuurlijk via internet. Er zijn diverse internetsites die aangeven waar je draadloze netwerken kunt vinden en of ze beveiligd of onbeveiligd zijn.

Afbeelding 3: Tekens bij warchalking

Opdracht 14

Hoeveel draadloze netwerken kun jij zien thuis? Hoe heten ze? Zijn ze beveiligd?

Opdracht 15

Wardrivers gebruiken speciale programma's om de draadloze netwerken te vinden. Zijn deze programma's verboden?

Opdracht 16

Wat is een hotspot?

12.6 Beveiligen

Gelukkig zijn er maatregelen die je kunt nemen om te voorkomen dat hackers jouw systeem binnendringen. Zoals bijvoorbeeld een firewall. Maar hoe gaan hackers te werk?
Je hebt al kunnen lezen dat hackers gebruik maken van exploits. De belangrijkste categorie van exploits is de buffer overflow. Tijd dus om ook eens te bekijken wat een buffer overflow is. Je zult merken dat hacken nog niet zo makkelijk is. Verder komt aan de orde hoe we het wardrivers moeilijker kunnen maken om je draadloze netwerk binnen te komen.

12.6.1 Firewall

Iedere computer in een netwerk heeft zijn eigen unieke Internet Protocol adres, het IP-adres. Om data naar een computer te kunnen sturen heb je zijn IP-adres nodig. Om er voor te zorgen dat de data bij het juiste programma terecht komt heeft elk IP-adres 65536 virtuele poorten. Als je bijvoorbeeld met een browser aan de slag gaat zullen de pagina's die je opvraagt via poort 80 (http) binnen komen. Het lezen van je mail gaat via poort 110 (pop3).
Een hacker maakt gebruik van deze poorten om een computer binnen te komen en met behulp van een poortscanner bekijkt de hacker alle poorten van een computer en controleert op deze manier of er een open staat.

Om een computer te beveiligen tegen hackers moeten we er voor zorgen dat er geen ongewenste bezoekers binnen komen, maar ook dat er niet zo maar informatie naar buiten gaat. Kortom we hebben een poortwachter nodig die al het verkeer, naar binnen en naar buiten, controleert en zo nodig blokkeert: een firewall. Met behulp van de firewall kun je poorten openen en afsluiten.

No.	Time	Source IP	Destination IP	Note	
1	11/14/2010 19:50:33	121.192.8.35:48967	192.168.1.50:80	ATTACK	syn flood TCP
2	11/14/2010 19:50:33	121.192.8.35:48961	192.168.1.50:80	ATTACK	syn flood TCP
3	11/14/2010 19:50:33	121.192.8.35:48959	192.168.1.50:80	ATTACK	syn flood TCP
4	11/14/2010 19:50:33	121.192.8.35:48951	192.168.1.50:80	ATTACK	syn flood TCP
5	11/14/2010 19:50:33	121.192.8.35:48955	192.168.1.50:80	ATTACK	syn flood TCP
6	11/14/2010 19:50:33	121.192.8.35:48950	192.168.1.50:80	ATTACK	syn flood TCP
7	11/14/2010 19:50:33	121.192.8.35:48952	192.168.1.50:80	ATTACK	syn flood TCP
8	11/14/2010 19:50:33	121.192.8.35:48953	192.168.1.50:80	ATTACK	

Afbeelding 4: Poortscan op poort 80.

Hier zie je een gedeelte van een log bestand van een webserver. De webserver heeft een intern IP adres (192.168.1.50) en wordt gescand op poort 80. Tussen de webserver en het internet bevindt zich de firewall en die heeft opdracht alle verzoeken richting poort 80 door te laten naar die webserver.

16	10/02/2010 10:05:49	195.241.77.55:53	192.168.1.35:62710	ATTACK	ports scan UDP
17	10/02/2010 10:05:47	195.241.77.58:53	192.168.1.35:62710	ATTACK	ports scan UDP
18	10/02/2010 10:05:45	195.241.77.58:53	192.168.1.35:55938	ATTACK	ports scan UDP
19	10/02/2010 10:05:44	195.241.77.55:53	192.168.1.35:55938	ATTACK	ports scan UDP
20	10/02/2010 10:05:35	195.241.77.58:53	192.168.1.35:53647	ATTACK	ports scan UDP
21	10/02/2010 10:05:21	195.241.77.58:53	192.168.1.35:53968	ATTACK	ports scan UDP

Afbeelding 5: Poortscan naar UDP poorten.

Opdracht 17

In afbeelding 4 en afbeelding 5 zie je een poortscan. Naar welke poortnummers wordt er gescand?

Opdracht 18

1. Wat is het verschil tussen een virusscanner en een firewall?
2. Waarom is het noodzakelijk dat een firewall ook het verkeer naar buiten in de gaten houdt?

Er zijn twee soorten firewalls: een hardware- en een softwarematige. De hardwarematige variant is een apart apparaat dat als firewall fungeert. Een softwarematige firewall slaat op een programma dat op de computer draait.

Opdracht 19

1. Stel dat je meerdere computers hebt in een netwerk, wat is dan het voordeel van een hardwarematige firewall ten opzichte van een softwarematige firewall?
2. In welk apparaat dat we al een keer zijn tegengekomen in dit lesmateriaal zit een firewall?
3. Noem een aantal programma's die je kunt gebruiken als softwarematige firewall?

Opdracht 20

Om je te beschermen tegen hackers is een firewall een oplossing. Computerbeveilingsbedrijven maken soms ook gebruik van de zogenaamde honeypots. Zoek uit wat honeypots zijn en hoe de beveiligingsbedrijven te werk gaan.

12.6.2 Buffer overflow

Een hacker kan dus door middel van een poortscanner controleren welke poorten open staan. Maar met een poortscanner is de hacker de computer nog niet binnen. De technieken die gebruikt worden om een computer binnen te komen, noemt men exploits. Er zijn sites waarop gevonden exploits te vinden zijn. Toch is hacken niet makkelijk. Om de exploits te begrijpen is veel kennis over computers nodig. En echte hackers gebruiken niet alleen exploits van anderen maar ontdekken zelf ook regelmatig nieuwe exploits.
De bekendste categorie van exploits is de buffer overflow. Om deze techniek te begrijpen moet we eerst weten wat een buffer is. Een buffer is een stukje geheugen in de computer dat wordt gebruikt voor tijdelijke opslag. Als je bijvoorbeeld een document afdrukt voordat je de printer hebt aangezet, worden de gegevens in de printbuffer gezet totdat de printer klaar is.
Als een hacker constant informatie naar een computer blijft sturen dan is het mogelijk dat de buffer overstroomt. Dit kun je vergelijken met een emmer die overstroomt als je er teveel water in laat lopen. Het programma krijgt meer gegevens te verwerken dan het eigenlijk aan kan. Een goed geschreven programma veroorzaakt bij een buffer overflow een foutmelding of een crash. Sommige

programma's voeren de commando's die buiten de buffer vallen toch uit. Van dit soort programma's maakt een hacker gebruik. De hacker laat de buffer overstromen en dwingt de computer om op het eind het door de hacker geschreven programma uit te voeren. Op deze manier kan een hacker de andere computer binnenkomen.

12.6.3 WiFi beveiligen

Als je wilt dat niemand op jouw draadloze netwerk (wifi) kan komen, moet je de draadloze verbinding beveiligen. Er zijn verschillende methodes om dit te doen.

12.6.3.1 Encryptie

Een methode om je netwerk veiliger te maken is het versleutelen van de gegevens die over het netwerk verstuurd worden. De gegevens zijn dan geheimtaal. Alleen als je de sleutel kent kun je de gegevens begrijpen. Weet je de sleutel niet dan kom je er niet op.
Er zijn meerdere typen sleutels, o.a. WEP en WPA.
WEP staat voor Wired Equivalent Privacy. In de router stel je de sleutel in. Als je met je laptop gebruik wilt maken van het basisstation heb je de sleutel nodig. Het nadeel van WEP is dat het redelijk eenvoudig te kraken is.
Een betere vorm van beveiliging is WPA (WiFi Protected Access). WPA maakt ook gebruik van een sleutel die je moet weten om op het netwerk te komen. Het verschil tussen WEP en WPA is dat bij WEP de sleutel is af te leiden uit de pakketjes die verstuurd worden. Bij WPA is het niet mogelijk om de sleutel af te leiden uit de verzonden pakketjes. De sleutel wisselt namelijk automatisch na enkele seconden. De nieuwste vorm van WPA is WPA-2. Die vorm van encryptie is nog veiliger.

12.6.3.2 MAC-filtering

Om op een netwerk aangesloten te zijn dan moet in je computer een netwerkkaart zitten. Elke netwerkkaart heeft een uniek nummer. Dit wordt het MAC-adres genoemd. In je basisstation van je draadloze netwerk kun je aangeven welke MAC-adressen welkom zijn op het netwerk.

Opdracht 21

1. Wat is het verschil tussen een IP-adres en een MAC-adres?
2. Wat is het MAC-adres van je netwerkkaart?
3. Heb je Windows ga dan via Bureau-accesoires naar Opdrachtprompt of je gaat via Start naar de opdrachtregel. Typ daarna ipconfig/all.
4. Bij Fysiek adres (Physical Address) kun je het MAC-adres van je netwerkkaart vinden. Kijk hier: http://www.ehow.com/how_5873875_mac-address-macbook-pro.html als je het MAC-adres op een Mac-book wilt vinden.
5. Wat is het IP-adres van je computer?

6. Je IP-adres kun je vinden met behulp van je browser. Ga naar de site watismijnip.nl. Het nummer dat je dan ziet is je IP-adres. Let wel, heb je thuis een netwerk dan zie je het IP-adres van jouw internetaansluiting waar de router op aangesloten zit maar niet het IP-adres van jouw computer. Die krijgt dan namelijk een intern adres dat meestal begint met 192.168. Via IP-config kun je het interne adres achterhalen.

Het nadeel van de MAC-filtering methode is dat er programma's zijn die het MAC-adres van een computer kunnen veranderen. Het nabootsen van een MAC-adres wordt spoofen (bedriegen) genoemd.

12.6.3.3 Zet de SSID uit

Elk draadloos netwerk heeft een naam. Dit is de SSID of Service of Set Identifier van het netwerk. Een wardriver is op zoek naar SSID's. Stel daarom in de router in dat dat je SSID niet wordt uitgezonden. Op deze manier kan een wardriver het netwerk minder goed vinden.

12.7 Ongewenste e-mail

Ongewenste e-mail kunnen we onderscheiden in:

- Spam
- Hoaxes
- Phishing

12.7.1 Spam

"SPAM" is een merknaam uit de voedselindustrie en staat voor ingeblikte ham. De makers van de Engelse televisieserie Monty Python gebruikten het in een sketch, die zich afspeelt in een café waarvan de menukaart vrijwel geheel uit gerechten met spam bestaat. Een groep Vikingen zingt voortdurend luidkeels: "Spam, spam, lovely spam, wonderful spam". Door het voortdurend gebruik van het woord spam wordt normaal converseren onmogelijk. Hierin zit de

overeenkomst met elektronische spam: door de toename van e-mail spam wordt normaal e-mailen ook steeds moeilijker.

Afbeelding 6: Spam

Behalve e-mailadressen, is het ook mogelijk om het internet te spammen. Dit kan bijvoorbeeld worden gedaan met een zogenaamde googlebom. Een googlebom is een methode om een bepaalde pagina hoog in de resultaten van Google te laten verschijnen terwijl de trefwoorden waar je op zoekt, niet eens voorkomen in de pagina. Probeer het maar eens met bijvoorbeeld de woorden "raar kapsel" of "miserable failure". Google bombing is mogelijk doordat Google niet alleen de frequentie van woorden op een pagina telt, maar ook het aantal links dat naar die pagina verwijst. Als veel mensen dus een link naar een bepaalde pagina plaatsen en daarbij trefwoorden gebruiken, dan zal Google deze pagina hoger ranken wanneer deze trefwoorden worden opgegeven in de zoekopdracht.
Naast SPAM bestaan er ook SPIM (ongewenste berichten via instant messaging) en SPIT (automatische oproep via de internettelefoon).

Opdracht 22

- Waarom versturen mensen spam?
- Hoe komt het dat mensen die spam versturen zo moeilijk op te sporen zijn?
- Is het versturen van spam strafbaar?
- Bedenk een goede Nederlandse vertaling voor het woord spam

12.7.2 Hoaxes

Een hoax is een nep waarschuwing. Meestal is het geschreven als een e-mailbericht. De e-mail probeert zich te verspreiden als een kettingbrief. Dit betekent dat in de boodschap de lezer wordt aangespoord om zoveel mogelijk mensen te informeren en de mail dus door te sturen. Het woord hoax komt uit het Engels, waar het zoveel betekent als nep, bedrog, truc of oplichterij.
Bekende voorbeelden van hoaxes zijn:

- November 2005
  heey iedereen, vanaf 1 november moet je gaan betalen voor je MSN en mail van hotmail, tenzij je dit mailtje doorstuurt naar 18 mensen. als je het niet gelooft kijkt dan op www.msn.com. als je dit naar 18 mensen doorstuurt wordt je MSN-poppetje blauw.
- Maart 2006
  Music Top 50, een nieuw tv-programma dat binnenkort op SBS6 komt, deelt gratis I-pods uit! Wanneer je dit mailtje doorstuurt naar ten minste 15 vrienden (of kennissen) krijg je een gratis I-pod thuisgestuurd. Je moet het mailtje ter controle ook naar bart@musictop50.com sturen, administratief medewerker Bart van Domburg die registreert wie er allemaal een gratis I-pods moeten

krijgen. Music Top 50 doet dit om aan meer naamsbekendheid te komen. Stuur je dit mailtje door naar 15 vrienden maak je dus reclame voor Music Top 50 en krijg je een gratis i-pod. Als je het zelfs doorstuurt naar 50 vrienden, dan krijg je alle singles uit de Top 50 bijgeleverd met I-pod! Stuur het door!

- Januari 2003
  Onderwerp: Waarschuwing voor virus !!
  We hebben een boodschap ontvangen van een van onze contacten dat ons adresboek wel eens geïnfecteerd kan zijn door een virus (genaamd jdbgmgr.exe) dat niet gedetecteerd wordt door de Norton of McAfee antivirus scanners. Het virus slaapt ongeveer een 14 dagen voordat het je computer gaat beschadigen. Het wordt automatisch doorgestuurd naar je contacten uit je adresboek, of je nu hen een e-mail stuurt of niet. Als het aanwezig is op uw PC is het mogelijk geïnstalleerd in c:\Windows\system.
  Wat moet u doen:
    - Ga in Windows Verkenners naar Extra, Zoeken, Bestanden of mappen, of gewoon in het start menu "zoeken" etc.
    - In het "Naam:" venster schrijft u "jdbgmgr.exe"
    - In het "Zoeken in:" venster gaat u naar "Drive_c (C:)"
    - Klik op "Nu zoeken"
    - Het virus heeft een klein beertje als icoon en de naam "jdbgmg.exe" OPEN DIT NIET !!!!!!!!!
    - Aanklikken met uw RECHTER muisknop en verwijderen (het gaat dan naar je Prullenbak)
    - Ga nu naar de Prullenbak en verwijder het bestand of maak de Prullenbak helemaal leeg
    - ALS U HET VIRUS VINDT, MOETEN ALLE ADRESSEN IN UW ADRESBOEK GEWAARSCHUWD WORDEN, OOK AL HEEFT U DE LAATSTE TIJD GEEN E-MAILS GESTUURD, ZIJ KUNNEN DAN OP HUN BEURT OOK HUN CONTACTEN WAARSCHUWEN.

- Een hoax herken je aan de volgende punten:
- Ze roepen op om het bericht door te sturen naar alle contactpersonen.
- Er wordt vaak gewezen op een groot gevaar of een beroep gedaan op medelijden.
- Er is overmatig gebruik gemaakt van leestekens.
- Er staan vaak spelfouten in.

Op de site http://www.virusalert.nl/?show=hoaxes kun je zien welke e-mailberichten hoaxes zijn. Gelukkig valt daar ook te zien dat het aantal hoax-en niet groot meer is.

Opdracht 23

Is het strafbaar als je een hoax verspreidt?

12.7.3 Phishing

Phishing is een variant op het Engelse woord fishing, wat "vissen" betekent.
Phishing is een vorm van oplichterij. Het doel van phishing is het verkrijgen van gevoelige informatie zoals creditcard nummers, wachtwoorden of inloggegevens. Een phisher doet zich meestal voor als een bekende organisatie, bijvoorbeeld een bank of online winkel. De phisher verstuurd miljoenen nep e-mails naar willekeurige mensen. In deze e-mail verzoekt de phisher de mensen om een site te bezoeken en er persoonlijke gegevens achter te laten. De link in het bericht verwijst echter niet naar de officiële site van de bank of winkel maar naar een vervalste website. Als een bezoeker van de nepsite dan zijn of haar gegevens invult, krijgt de phisher ze op een presenteerblaadje aangereikt.
Veel voorkomende zinnen in een phishing e-mail zijn:

- "Geachte klant."
- "Controleer uw account."
- "Klik op de onderstaande link om toegang te krijgen tot uw account."

Vaak is de boodschap van de mail dat het bedrijf de klantgegevens aan het bijwerken is. Daarom moeten klanten opnieuw inloggen. Maar let op: een bank of internetbedrijf zal nooit om persoonlijke gegevens vragen via een e-mail. Dus als je zo'n e-mail binnenkrijgt dan kun je deze het beste meteen weggooien.
In afbeelding 7 een voorbeeld van een phishing e-mail:

Afbeelding 7: Een phishing mail. Kijk eens goed naar het mail adres bovenin!

Opdracht 24

- Wat is het doel van phishing?
- Wat kun je het beste doen met een phishing e-mail?

12.7.4 Spamfilters

Men schat dat tegenwoordig bijna 90 procent van de e-mails die worden verzonden spam is. Daarom wordt er erg veel gedaan aan het bestrijden van spam. Een manier om dit te doen is gebruik te maken van spamfilters. Als gebruiker heb je dan weinig last van de spam, omdat die er voor je uit wordt gefilterd. Maar hoe werkt dat filteren precies?
De makkelijkste manier om mail te filteren is gebruik maken van een woordfilter. Alle berichten die binnenkomen, worden door de computer gescand. Als er een bepaald woord uit het woordfilter in voorkomt (bijvoorbeeld viagra), dan bestempelt de computer het bericht als spam.
Woordfilters kunnen werken met verboden woorden, zoals hierboven, en ook met toegestane woorden. Door te tellen hoeveel toegestane en verboden woorden een bericht bevat, kan de computer bepalen of een bericht wel of geen spam is. Dit heet een heuristisch filter. Zo'n filter bepaalt eigenlijk de kans dat een bericht spam is.

Nog slimmer is het om niet vaste woordenlijsten te gebruiken, maar de woordenlijsten steeds aan te passen. In zo'n geval wordt een spamfilter Bayesiaans genoemd. Bayesiaanse filters moeten worden getraind. Dit betekent, dat je het filter van tevoren moet vertellen welke berichten wel spam zijn, en welke berichten geen spam zijn. Het programma scant dan alle berichten, en maakt een lijst van alle woorden die in die berichten voorkomen. Voor elk woord wordt geteld in hoeveel spamberichten het voorkomt, en in hoeveel niet-spamberichten het voorkomt.

12.7.5 E-mailadressen

Ongewenste e-mail kan alleen maar verstuurd worden als bedrijven weten waar ze het naar toe moeten sturen. Hoe komen spammers nu aan deze e-mailadressen? Als je weet hoe bedrijven aan je e-mailadres komen dan weet je ook gelijk hoe je dit kunt voorkomen.
Er zijn verschillende manieren om aan e-mailadressen te komen. De eerste manier waarop spammers aan adressen kunnen komen is door gebruik te maken van een zogenaamde spider. Een spider is een programma dat het hele internet afzoekt naar @ symbolen. Dus op elke pagina die de spider tegenkomt zoekt hij naar het @-symbool. De spider slaat het woord voor en na het apenstaartje op in een bestand en zo vindt de spider een hoop e-mailadressen. Spiders zijn krachtige programma's dus als je geen ongewenste e-mailberichten wilt kun je het beste je e-mailadres geheim houden en het in ieder geval niet op internet zetten.

Opdracht 25

- Kijk eens op de pagina van Tanenbaum (http://www.few.vu.nl/~ast/). Hoe heeft hij dit mailadresprobleem opgelost?
- Bedenk nog een oplossing om toch je e-mailadres op het internet te kunnen plaatsen zonder dat een spider het kan vinden

Een tweede manier waarop spammers aan adressen komen is door te gokken. Er bestaan computerprogramma's die miljoenen adressen kunnen genereren: zoals jan1@hotmail.com, jan2@hotmail.com enzovoort. Zorg ervoor dat, als je een nieuw e-mailadres aanmaakt, je niet een standaard e-mailadres neemt maar een e-mailadres dat moeilijk te raden is door dit soort programma's. Spammers hoeven niet eens zelf deze programma's te gebruiken. Er zijn op internet dvd's te koop vol met e-mailadressen.

Opdracht 26

Probeer op internet een site vinden waarop je dvd's met e-mailadressen kunt kopen.

12.7.6 Captcha

Afbeelding 8: Een captcha

Als je een spam of phishing bericht wilt sturen, wil je dat natuurlijk niet van je gewone e-mailadres doen. Je wilt liever anoniem zijn. Daarom schakelen professionele spammers programma's in om heel veel e-mailaccounts aan te maken bij een gratis webmaildienst zoals Hotmail of Gmail. Een computerprogramma dat dit automatisch kan doen wordt een bot genoemd. Een bot kan ook gebruikt worden om op gastenboeken of weblogs reclame achter te laten. Bots zijn voor spammers dus heel krachtige programma's die veel werk in korte tijd kunnen doen.
Om te voorkomen dat een bot automatisch een formulier kan invullen, kan op dat formulier gebruik gemaakt worden van een captcha. Wat is het en waarom is het nuttig?
Captcha is een afkorting voor "Completely Automated Public Turingtest to tell Computers and Humans Apart". Met een captcha kan bepaald worden of er sprake is van een menselijke gebruiker. Een bekend voorbeeld van een captcha zie je in afbeelding . Het is de bedoeling dat je de tekst overtypt. Pas als je de tekst goed overtypt kan je het formulier inleveren. Een bot heeft heel veel moeite om de teksten te lezen.
Hoewel Captcha's nog veel worden gebruikt, werken ze niet meer zo goed als vroeger. De bots worden steeds slimmer en met behulp van patroonherkenning is het mogelijk voor de bots om de captcha's te lezen.

Wil je ook een captcha op jouw website? Kijk dan eens bij reCaptcha (http://www.google.com/recaptcha). Hiermee krijg je niet alleen een captcha op jouw site maar helpt iedere gebruiker ook nog eens mee boeken te digitaliseren!

12.7.7 Spoofing

Tenslotte nog iets over spoofing. Spoof is Engels voor bedrog, bedrieglijke nabootsing van iets. Spammers en phishers maken gebruik van deze techniek.
In een phishing mail wordt vaak verwezen naar een nagemaakte website. Er wordt meestal gebruik gemaakt van URL-spoofing. Dit is het nabootsen van een bekend

internetadres zodat de gebruiker denkt de echte site te bezoeken, terwijl de website die van de bedrieger is. Bijvoorbeeld:
http://www.google.nl i.p.v. http://www.google.nl

Opdracht 27

Kun jij het verschil vinden tussen de twee schrijfwijzen van de websites van Google? (De adressen lijken hier hetzelfde maar selecteer ze maar eens en kopieer en plak ze eens in een tekstverwerker met als lettertype Courier. Dan zie je het verschil wel.)

Niet alleen het internetadres lijkt op de echte site, ook de opmaak van de website lijkt vaak erg op die van de echte site. Het is dus niet makkelijk te ontdekken dat je als bezoeker op een gespoofde site zit.
Zorg ervoor dat als je betrouwbare informatie van jezelf (bijvoorbeeld een wachtwoord) intypt dat er gebruik is gemaakt van een beveiligde site. Een beveiligde website maakt gebruik van een SSL certificaat. SSL staat voor Secure Sockets Layer en beveiligt data tegen onderschepping door derden door middel van een codering (encryptie). Een SSL beveiligde website is te herkennen aan:

https:// voor het internetadres en een slotje in de balk bij Opera: 

Een slotje en in het groen **https://** bij Google Chrome: 

Of **https://** en een simpel slotje bij Firefox: 

Opdracht 28

Bekijk hoe bij Internet Explorer en Safari aangegeven wordt dat je je op een SSL beveiligde website bevindt.

Moderne browsers hebben tegenwoordig allemaal een phishing-filter. Dit controleert of sites betrouwbaar zijn.

12.7.8 OpenSSL en heartbleed

Maar ook het slotje is niet altijd een teken dat een website betrouwbaar is.
Voor het benaderen van een website met een SSL certificaat wordt vaak gebruik gemaakt van een bibliotheek met software om deze beveiliging te implementeren. OpenSSL is zo'n bibliotheek. OpenSSL wordt veel gebruikt in de beveiliging van onder meer webwinkels en routers. In Nederland

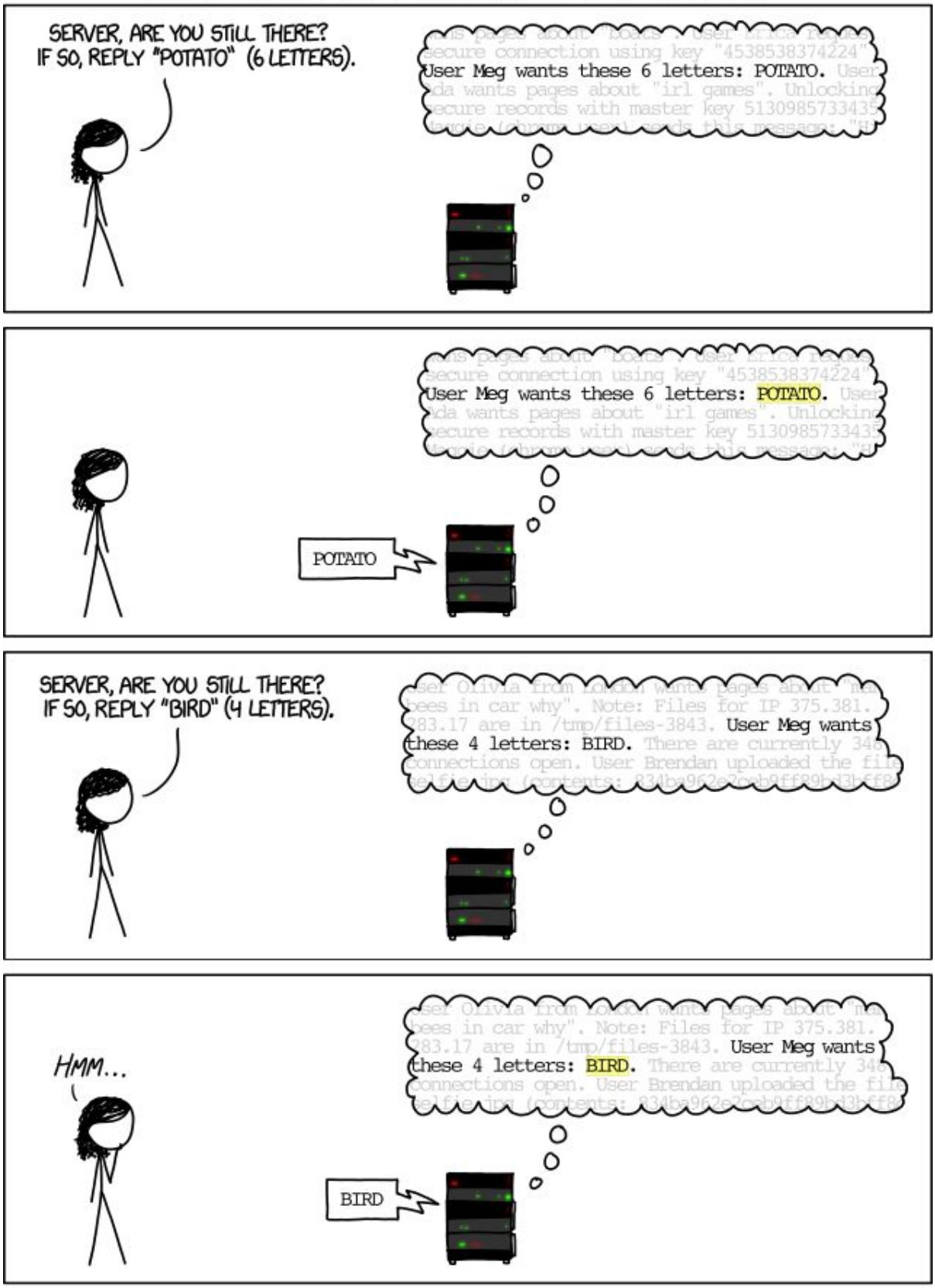
maakt onder andere de iDEAL-betaalmethode er gebruik van.
OpenSSL is een open source project dus er werken wereldwijd mensen aan mee om deze te onderhouden.
Op 31 december 2011 werd een bijdrage van een van de programmeurs toegevoegd waarin een fout zat. Het ging om een onderdeel dat Heartbeat genoemd werd.
Deze fout maakt het mogelijk om een speciaal verzoek naar een ‘beveiligde’ server te sturen zodanig dat die server een min of meer willekeurig deel van zijn geheugen, ter grootte van maximaal 64 kB, terugstuurt. Dit geheugen kan gebruikersnamen en wachtwoorden bevatten maar ook sleutels van beveiligingscertificaten. Dit laatste maakt bijvoorbeeld man-in-the-middle-aanvallen mogelijk, waarbij een kwaadwillende website zich kan uitgeven voor een officiële website zonder dat de gebruiker dit merkt.

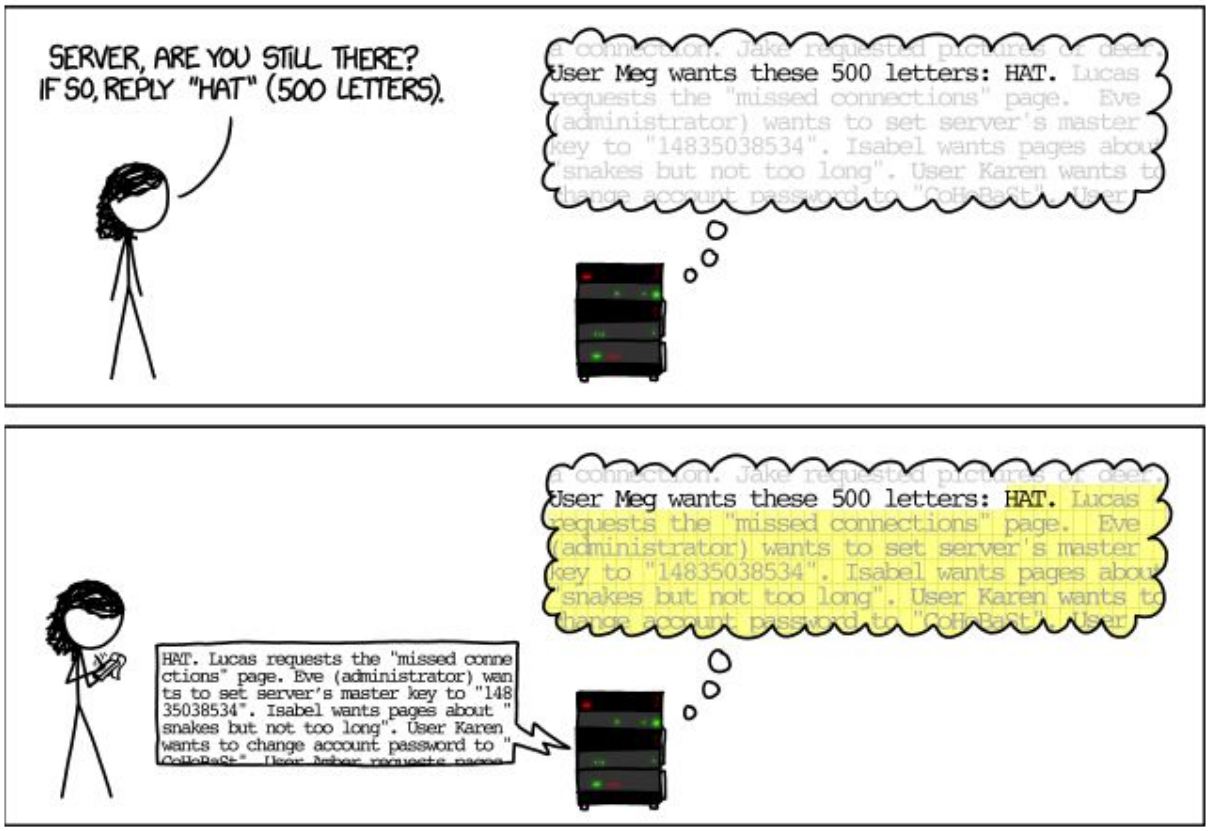
Het lek werd ontdekt door Neel Mehta van Google Security en op 7 april 2014 bekend gemaakt door het OpenSSL Project nadat een selecte groep grote organisaties, onder andere Google, Yahoo!, Facebook en Microsoft, eerder een kans had gekregen het lek op hun servers te dichten. Op 7 april is versie 1.0.1g van OpenSSL uitgebracht, waarin deze fout niet meer voorkomt. Veel populaire websites moesten daarna hun gebruikers adviseren hun wachtwoorden te veranderen.

Opdracht 29

Wat is een man-in-the-middle aanval?

HOW THE HEARTBLEED BUG WORKS:





12.7.9 Stopt het ooit?

Sinds april 2014 wordt Windows XP niet meer ondersteund door Microsoft. Dat houdt o.a. in dat er in de software geen lekken meer gedicht worden. Iemand suggereerde dat Windows XP ondertussen wel zo volwassen zou zijn dat alle lekken er wel uit zijn. In reacties werd gesuggereerd dat hackers misschien wel al ontdekte fouten nog niet zouden gebruiken maar daarmee wachtten tot Microsoft zou stoppen met de ondersteuning. Want daarna hadden ze een lek dat nooit meer gedicht zou worden.

Het onderstaande artikel van 2 mei 2014, afkomstig van nu.nl, geeft al aan dat het nooit stopt.

'Beveiligingslek maakt imiteren grote websites mogelijk'

Er is opnieuw een groot beveiligingslek ontdekt in een protocol dat wordt gebruikt om veel grote websites veilig te houden.

Het probleem treft de opensourcesoftware OAuth en OpenID, stelt de Singaporese onderzoeker Wang Jing tegenover *Cnet*.

De bug maakt het voor aanvallers mogelijk om een popup-bericht van populaire sites na te maken. Bij het klikken op een link is het bijvoorbeeld mogelijk om een nep-inlogscherm van Facebook te tonen, waarmee apps aan het sociale netwerk gekoppeld zouden kunnen worden.
In de browserbalk staat dan ook daadwerkelijk het webadres van Facebook, maar bij het verzenden van gegevens worden deze naar de aanvaller gestuurd, in plaats van naar het sociale netwerk. Ook kan de gebruiker worden doorgestuurd naar een webpagina van de hacker.

Vanuit phishing-e-mails worden mensen nu vaak ook al doorgestuurd naar nepversies van populaire sites, maar in de adresbalk van de browser is dan normaal gesproken te zien dat de gebruiker zich eigenlijk op een andere site bevindt.

Reacties

Het lijkt niet makkelijk om de bug op te lossen, omdat dan het risico ontstaat dat apps die niet kwaadaardig zijn ook worden geblokkeerd. Vertrouwde apps zouden allemaal op een 'witte lijst' moeten komen. Volgens Wang zegt Facebook dan ook dat het probleem niet op de korte termijn zal worden verholpen. Wel zeggen Facebook, Google, Microsoft en Linkedin de kwetsbaarheid in de gaten te houden. Gebruikers die niet via popup-vensters inloggen op sociale netwerken, lopen geen gevaar door het lek.

De bug volgt op het serieuzere Heartbleed-lek, dat ook veel grote websites trof via de beveiligingssoftware OpenSSL. Door dat lek kwamen veel meer gegevens in gevaar en werden internetgebruikers aangeraden hun wachtwoorden te veranderen.

12.8 Cryptografie

Cryptografie houdt zich bezig met het omzetten van een bericht of bestand in geheimtaal. Het voordeel hiervan is dat pottenkijkers niet meer mee kunnen lezen. Alleen de ontvanger, die de beschikking heeft over de juiste sleutel, kan uit het geheimschrift de originele boodschap terugkrijgen. Cryptografie wordt tegenwoordig veel toegepast. Bijvoorbeeld in gsm's, pin-automaten, de chipknip of de decoder van de TV. Cryptografie wordt ook gebruikt om bestanden te versleutelen, e-mails te coderen of om afgeschermde websites mee te bekijken. Een voorbeeld van dit laatste punt zijn de SSL-certificaten uit het hoofdstuk ongewenste e-mail. In dit hoofdstuk houden we ons vooral bezig met het versleutelen van e-mailberichten. Welke mogelijkheden zijn er om je e-mailberichten te vertalen in geheimtaal zodat niemand mee kan lezen?

Drie belangrijke begrippen in de cryptografie zijn:

- ***Encryptie***: het versleutelen van de informatie door de zender
- ***Decryptie***: het weer ontcijferen van de informatie door de ontvanger
- ***Sleutel***: De sleutel wordt gebruikt om de informatie te encrypten en ook om de informatie te decrypten

12.8.1 Simpele methodes

Julius Caesar was de eerste die op vrij grote schaal gebruik maakte van cryptografie. Hij gebruikte geheimschrift om zijn leger te informeren. De methode die Julius Caesar gebruikte is een van de simpelste vormen van cryptografie en werkt als volgt:
Elke letter in een bericht werd in het alfabet 3 plaatsen opgeschoven Dus een A werd een D. Een B werd een E enzovoort. Een X werd weer een A.

De methode van Julius Caesar is te makkelijk te kraken en wordt niet meer gebruikt in de cryptografie. In de Tweede Wereldoorlog dachten de Duitsers na over een betere encryptie methode en kwamen met de Enigma. De Enigma is een soort typemachine die uit 3 onderdelen bestaat: drie code-wielen, het toetsenbord en een paneel met lampen waarbij elke lamp bij een letter hoort.

Afbeelding 9: De enigma

Eerst moest een begin-instelling van de enigma gekozen worden. Deze begin-instelling werd uit een codeboek gehaald waar voor elke dag een andere instelling stond. Daarna kon de boodschap ingetoetst worden. De drie code-wielen

vertaalden elke letter drie keer naar een geheime letter die werd aangegeven op het paneel van lampen. Het voordeel van deze methode was dat na elke letter de code-wielen draaiden. Een letter W werd dus elke keer in een andere geheime letter vertaald. Het nadeel van deze methode was dat iedereen die de berichten wilden ontcijferen hetzelfde codeboek voor de begin-instelling moesten hebben. Deze codeboeken moesten dus verspreid worden over het hele Duitse leger. Uiteindelijk werd de code van de Enigma toch gekraakt door de Polen en de Britten.
Ook de Enigma wordt niet meer gebruikt in hedendaagse cryptografie. Tegenwoordig heb je een betere beveiliging nodig.

12.8.2 RSA

De voorbeelden die we tot nu toe gezien hebben zijn voorbeelden van symmetrische cryptografie. Dit betekent dat je dezelfde sleutel nodig hebt voor het encrypten en decrypten van een bericht. Het probleem hiervan is dat je de sleutel moet doorgeven en hierdoor kan deze onderschept worden. De onderschepper kan de berichten dan meelezen.
Tegenwoordig wordt daarom gebruikt gemaakt van asymmetrische cryptografie. Bij asymmetrische cryptografie heeft men twee verschillende sleutels: een sleutel om de informatie te encrypten en een andere sleutel om de informatie te decrypten.
De meest bekende encryptie methode tegenwoordig is RSA. Deze methode maakt gebruik van asymmetrische cryptografie en van priemgetallen. Dit maakt de RSA methode heel veilig. RSA is genoemd naar de initialen van de uitvinders: Rivest, Shamir en Adleman.
De RSA methoden maakt gebruik van priemgetallen. Elk heel getal kan worden gemaakt door bepaalde priemgetallen met elkaar te vermenigvuldigen. En dat kan maar op één manier. Zo kun je het getal 42 maken door de priemgetallen 2,3 en 7 met elkaar te vermenigvuldigen (2 * 3 * 7 = 42). Er is geen andere combinatie van priemgetallen mogelijk die je met elkaar kunt vermenigvuldigen en die 42 oplevert.
RSA maakt gebruik van deze eigenschap van priemgetallen. Zoals we al eerder hebben gezien maakt RSA gebruik van twee sleutels: een publieke sleutel en een geheime sleutel. De publieke sleutel mag iedereen weten en deze sleutel is nodig om een bericht te encrypten. De geheime sleutel moet je goed geheim houden en met behulp van deze sleutel kun je een bericht decrypten. De publieke sleutel kun je maken door 2 priemgetallen met elkaar te vermenigvuldigen. Bijvoorbeeld 2027 * 6359 = 12889693. De publieke sleutel is dus nu 12889693. Met deze sleutel kun je een bericht encrypten.
Om het bericht vervolgens te decrypten heb je de getallen 2027 en 6359 nodig. Het is niet makkelijk om erachter te komen welke priemgetallen je met elkaar moet vermenigvuldigen om de publieke sleutel te krijgen. Bij kleine getallen lukt dit nog

wel maar bij heel grote getallen is dit met de huidige computers niet mogelijk. Dus als je een bericht veilig wil versturen heb je een heel grote publieke sleutel nodig.

12.9 De wet

Sinds 1993 bestaat er in Nederland een wet om computercriminelen aan te pakken. In deze nieuwe wet werden onder andere computervredebreuk, virusverspreiding, gegevensbeschadiging, het onbevoegd aftappen van gegevensverkeer en het vervalsen van betaalpassen strafbaar gesteld. Deze wet heet de wet computercriminaliteit I.
De Wet uit 1993 bleek snel verouderd door de snelle ontwikkelingen op computergebied. Daarom is per 1 september 2006 de Wet computercriminaliteit II ingegaan. In dit hoofdstuk zullen we een aantal artikelen uit de wet computercriminaliteit II bekijken.

12.9.1 Computervredebreuk (hacken)

De bekendste vorm van computercriminaliteit is inbreken in een computersysteem. De wet noemt dit computervredebreuk. Met het wetsartikel 138 kunnen hackers bestraft worden. Onder de oude wetgeving was computervredebreuk alleen strafbaar wanneer een beveiliging werd doorbroken. Deze eis is komen te vervallen. Computerinbraak is nu strafbaar wanneer de dader wist of had kunnen weten dat hij op verboden terrein was. In Nederland zijn er nog niet zoveel mensen veroordeeld voor het plegen van computervredebreuk.

Een paragraaf uit een wetsartikel wordt een lid genoemd.
Hieronder staan 2 leden uit **Artikel 138a.**

- Lid 1 Hierin is vastgelegd dat het inbreken in iemand anders zijn computer strafbaar is. Straf: Gevangenisstraf van ten hoogste een jaar of geldboete van 16750 euro.
- Lid 2 Wie na het opzettelijk binnendringen ook nog eens gegevens kopieert, kan een straf van maximaal vier jaar cel krijgen

Om een computer binnen te dringen wordt vaak gebruik gemaakt van software.
Artikel 139 zegt over deze software:

- Lid 2a Het maken, vervaardigen, verkopen, verwerven, invoeren, verspreiden of anderszins ter beschikking stellen of voorhanden hebben van dergelijke software is een strafbaar feit. Straf : 1 jaar cel of een boete van 16.750 euro.

Sinds september 2006 is er niet alleen een artikel 138a maar ook een **artikel 138b**.
In dit artikel staat:

- Het is niet toegestaan een systeem plat te leggen door er grote hoeveelheden data naar toe te sturen. Straf : maximaal 1 jaar cel of geldboete van 16.750 euro

Met behulp van deze nieuwe wet is het nu mogelijk om het uitvoeren van een denial of service aanval (DOS-aanval, ook wel verstikkingsaanval genoemd) te bestraffen.

Opdracht 30

- Kan een hacker met goede bedoelingen bestraft worden?
- Vind jij dat een hacker met goede bedoelingen bestraft moet worden? (geef argumenten)
- Hoeveel jaar kun je maximaal krijgen als je als wardriver niet alleen op zoek bent naar draadloze netwerken maar ook inlogt op een onbeveiligd draadloos netwerk en gebruik maakt van de internetverbinding?
- Zoek op wat een zombie is. Op grond van welk lid van dit artikel kan een persoon die een zombie misbruikt bestraft worden?
- Stel dat je zoveel spam verstuurt dat de servers het niet meer aankunnen, hoe kan je dan gestraft worden?

12.9.2 Gegevensbeschadiging

Een ander belangrijk wetsartikel in de computerwetgeving is **artikel 350a**.
Hierin staat dat het verboden is om opgeslagen gegevens te vernielen:

- Lid 1: Het is verboden om gegevens te veranderen, wissen of toe te voegen.
  Straf: twee jaar cel of een boete van 16.750 euro
- Lid 2: Lid 2 zegt dat er nog een extra straf is voor degenen die eerst in een computer inbreken voordat ze gegevens wijzigen.
  Straf: vier jaar cel of een boete van 16.750 euro
- Lid 3: Het verspreiden van virussen, wormen of Trojaanse paarden is verboden
  Straf: maximaal vier jaar cel
- Lid 4: Lid 3 mag wel als als de verspreider goede bedoelingen heeft.

De eerste persoon die in Nederland veroordeeld is voor het schrijven van een virus was Jan de W. in het jaar 2001. Hij maakte Het Kournikova-virus met behulp van een virusmaker die hij gedownload had van internet. Het Kournikova virus was een van de meest verspreide virussen in 2001.

Een artikel dat lijkt op het artikel 350a is **artikel 161sexies**:

- Lid 1: Het is verboden om opzettelijk een computersysteem te vernielen, beschadigen of onbruikbaar te maken. Met het vernielen van een computer wordt niet het fysiek vernielen van een computer bedoeld.
  Straf: een jaar cel
  Straf: zes jaar cel als goederen of diensten in gevaar worden gebracht
  Straf: negen jaar cel als er levensgevaar door wordt veroorzaak
  Straf: vijftien jaar cel als er iemand door komt te overlijden

Opdracht 31

- Noem een voorbeeld van lid 4 van artikel 350a
- Wat is defacen? Op grond van welk lid van dit artikel kan een persoon die defacet bestraft worden?
- Wat is ransomware? Op grond van welk lid van dit artikel kan een persoon die ransomware gebruikt bestraft worden?
- Het plaatsen van spyware is alleen strafbaar als iemand hiervoor inbreekt in je computer. Er is echter ook spyware die legaal op je computer geplaatst wordt en dus niet bestraft kan worden. Op welke manier kan er legaal spyware op je computer geplaatst worden? (Hint : zoek op Google op de woorden spyware en legaal)
- Kan het sturen van een hoax bestraft worden onder artikel 350?

Opdracht 32

Wouter heeft leuke films gekocht in de winkel en wil deze films delen met zijn vriend Jasper. Een mogelijkheid om bestanden te delen is met een FTP-server. FTP staat voor File Transfer protocol. Wouter installeert op zijn computer thuis een FTP-server waarop alleen Jasper kan inloggen. Jasper logt in op de FTP-server en downloadt alle leuke films van Wouter.

- Overtreedt Wouter de wet? Waarom wel/niet?
- Overtreedt Jasper de wet? Waarom wel/niet?

Opdracht 33

Danny komt bij een poortscan een open poort tegen op de computer van Linda. Danny komt de computer makkelijk binnen en kijkt even rond wat Linda allemaal heeft. Hij doet verder niets en laat de computer weer met rust.
Overtreedt Danny de wet? Waarom wel/niet?

Opdracht 34

Annelies heeft een website gemaakt over haar favoriete artiest. Op deze website heeft ze ook stukjes muziek geplaatst.
Overtreedt Annelies de wet? Waarom wel/niet?

12.10 RFID chips

Radio Frequency Identification (RFID) is een automatische identificatiemethode. Een RFID chip is een minuscule chip die je ergens op kunt plakken of aan kunt hangen (bijvoorbeeld aan dingen, mensen of dieren). Een RFID lezer kan draadloos de informatie uit de chip halen. Elke chip heeft een unieke code. Omdat er relatief veel informatie op een RFID chip kan, ze geen batterij nodig hebben en ze goedkoop gemaakt kunnen worden, worden RFID chips nu al veel toegepast. In de toekomst zal dat alleen maar meer gaan worden.

Hieronder staan enkele toepassingen waar de RFID chip nu al gebruikt wordt in Nederland:

- Baja beach club: RFID chips worden gebruikt in de Rotterdamse discotheek Baja Beach Club. Een vaste klant met een RFID chip in zijn arm kan op deze manier afrekenen. Een chipknip in je arm dus.
- Bibliotheekboeken : Alle bibliotheekboeken in Nederland bevatten een chip. Hierdoor kunnen ze makkelijker uitgeleend en gevonden worden.
- Paspoorten: Alle Europese paspoorten die na augustus 2006 zijn uitgegeven bevatten een chip. Op deze chip staan al je gegevens en zelfs je foto. Dit is om fraude tegen te gaan.
- Dieren: Denk maar aan de gele oormerken van de koeien. Hierin zitten RFID chips. Maar ook honden en katten worden gechipt.
- Bagage: Schiphol wil alle koffers uitrusten met een RFID chip. De bagage blijkt zo namelijk veel beter te volgen. Dit project is nog in de testfase.
- OV-chipkaart: Deze bevat ook een RFID-chip. Op deze manier kunnen mensen reizen met de metro, tram of bus en wordt de oude strippenkaart overbodig.
- WK-voetbal :Tijdens het Wereldkampioenschap voetbal van 2006 zijn in de toegangskaarten RFID-chips verwerkt. Op deze manier waren de kaarten veel moeilijker na te maken.

Deze nieuwe techniek is heel handig maar brengt ook problemen met zich mee. Op de VU in Amsterdam hebben ze het eerste virus geschreven voor een RFID-chip. Dit heeft toen wereldwijd het nieuws gehaald.

Een nadeel van virussen op de chips wordt beschreven in het volgende scenario:

Een persoon komt een supermarkt binnen en koopt een pot pindakaas met een RFID chip. Thuis aangekomen haalt hij de chip van de pot af en hij plakt een nieuwe met een virus geïnfecteerde chip terug op de pindakaas. Hij neemt de pot pindakaas weer mee naar de supermarkt en rekent deze opnieuw af. Als de pot pindakaas nu gescand wordt dan wordt het supermarkt systeem geïnfecteerd met een virus. Dit kan een hoop problemen tot gevolg hebben, bijvoorbeeld dat alle prijzen van de producten veranderen. Supermarkten gebruiken nu nog geen RFID chips maar streepjescodes. Ze zijn wel van plan om over te stappen omdat RFID scanners veel sneller zijn.

Opdracht 35

Open de volgende pagina:
http://www.volkskrant.nl/vk/nl/2686/Binnenland/article/detail/775643/2006/03/15/Vervanger-streepjescode-vatbaar-voor-virussen.dhtml
en bekijk het artikel. Op de afbeelding in dat artikel staat een voordeel van het gebruik van RFID-chips op de boodschappen. Wat is dit voordeel?