Hacker Highschool
SECURITY AWARENESS FOR TEENS

LES 9
E-MAIL BEVEILIGING

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

Informatie over de “Gebruiksvoorwaarden”

De lessen en werkboeken van het Hacker Highschool (HHS) project zijn beschikbaar onder de volgende door ISECOM gestelde voorwaarden:

Alle informatie uit het HHS-project mag, niet-commercieel, gebruikt worden voor en door basisschool-leerlingen en studenten van middelbaar en hoger onderwijs. Dit materiaal mag niet worden gereproduceerd voor (door-)verkoop in welke vorm dan ook. Gebruik van dit materiaal in een klas, cursus, training, kamp of andere georganiseerde vorm van kennisoverdracht waarvoor geld wordt gevraagd is expliciet verboden zonder een licentie. Om een licentie te regelen kunt u het onderdeel LICENSE bezoeken op de website van de Hacker Highschool, www.hackerhighschool.org/license.

Het HHS-project is een leermiddel en, zoals met elk leermiddel, de docent/trainer bepaalt in grote mate het effect van het leermiddel. ISECOM kan geen aansprakelijkheid aanvaarden voor de positieve of negatieve gevolgen van het gebruik van dit materiaal en de daarin opgenomen informatie.

Het HHS-project is een initiatief van de open community, en wanneer u de resultaten van onze inspanning waardevol genoeg vindt om het te gebruiken, vragen we u uw steun te betuigen door:

- de aankoop van een licentie;
- een donatie
- ons te sponsoren.

Inhoudsopgave

Auteurs

Stephen F. Smith, Lockdown Networks

Chuck Truett, ISECOM

Marta Barceló, ISECOM

Kim Truett, ISECOM

Translation by Raoul Teeuwen

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

9.0 Introductie

Iedereen gebruikt e-mail. Het is de op één na meest gebruikte applicatie op het internet, na de webbrowser. Maar wat je wellicht niet weet is dat een aanzienlijk deel van alle netwerkaanvallen en inbraken voortkomen uit e-mail. En met betrekking tot je privacy, misbruik van e-mail kan potentieel de inhoud van je bericht zichtbaar maken, of een spammer informatie over jou geven. Het doel van deze module is je informatie geven over hoe e-mail werkt, veilig e-mail gebruik, e-mail gebaseerde aanvallen en beveiligingsstrategieen voor e-mail.

9.1 Hoe E-mail Werkt

Net zoals luchtpost door de lucht wordt verstuurd, wordt 'e'-mail door de 'e' gestuurd – waarbij de 'e' in dit geval het web of electronische verbindingen in en tussen netwerken zijn die het internet vormen. Wanneer je een e-mail verstuurd vanaf je computer wordt de data door je computer naar een SMTP server gestuurd. De SMTP server zoekt vervolgens naar de goede POP3 server en stuurt je e-mail naar die server, waar het wacht totdat het wordt opgehaald door de beoogde ontvanger.

9.1.1 E-mail Accounts

E-mail accounts zijn beschikbaar bij veel verschillende bronnen. Misschien krijg je er 1 van school, van je werk, of van je ISP. Als je een e-mail account krijgt, krijg je een twee-delig e-mail adres, in het volgende formaat: *gebruikersnaam@domein.naam*. Het eerste deel, *gebruikersnaam,* identificeert je op je netwerk, zodat je binnen dat netwerk verschilt van alle andere gebruikers op dat netwerk. Het tweede deel, *domein.naam*, wordt gebruikt om je specifieke netwerk te identificeren. De gebruikersnaam moet uniek zijn binnen je netwerk, net zoals de domeinnaam uniek moet zijn voor alle netwerken op het internet. Maar gebruikersnamen zijn niet perse uniek buiten hun netwerk; het is dus mogelijk dat twee gebruikers op twee verschillende netwerken dezelfde gebruikersnaam hebben. Bijvoorbeeld, als er een gebruiker met het adres *bill@bignetwork.net* is, zal er op *bignetwork.net* niet nog een gebruiker met de naam *bill* zijn. Maar *bill@bignetwork.net* en *bill@smallnetwork.net* kunnen we beiden bestaan en naar verschillende gebruikers leiden.
Eén van de eerste dingen die je doet als je je e-mail-account inricht, is je e-mail-adres invoeren in de e-mail-client. Je e-mail-client is het programma waarmee je e-mail verstuurt en ontvangt. Denk aan het populaire (want gratis met het besturingssysteem van Microsoft meegeleverde)Outlook Express van Microsoft, maar er zijn er veel meer, zowerl voor Windows als Linux, zoals Eudora, Mozilla Thunderbird en Pine.

9.1.2 POP en SMTP

Nadat je je e-mail-client hebt verteld wat je e-mail-adres is, moet hij weten waar hij moet kijken voor ontvangen e-mail, en waar uitgaande e-mail naartoe moet.
Je inkomende e-mails zullen zich bevinden op een computer die *POP server* wordt genoemd. De POP server – vaak met een naam als *pop.smallnetwork.net* of *mail.smallnetwork.net* – bevat een bestand die gelinked is aan je e-mail-adres en waarin de e-mails staan die iemand aan jou heeft gericht. *POP* staat voor *post office protocol*.
Je uitgaande e-mails worden verstuurd naar een computer die SMTP *server* heet. Deze server – met de naam *smtp.smallnetwork.net* – zal kijken naar de *domeinnaam* in het e-mail-adres van elke door jou verstuurde e-mail, zal vervolgens een *DNS lookup* uitvoeren om te bepalen bij welke POP3 server hij de e-mail moet afleveren. *SMTP* staat voor *simple mail transfer protocol*.
Wanneer je je e-mail client start, gebeuren er een aantal dingen:
1. de client opent een netwerkverbinding naar de POP server
2. de client stuurt je geheime wachtwoord naar de POP server
3. de POP server stuurt alle binnengekomen mail naar je lokale computer
4. de client stuurt alle uitgaande e-mail naar de SMTP server.

Het eerste wat opvalt, is dat er geen wachtwoord wordt gestuurd naar de SMTP server. SMTP is een oud protocol, ontworpen in de begindagen van de e-mail, in een tijd waarin bijna iedereen op het internet elkaar persoonlijk kende. Het protocol was geschreven met de veronderstelling dat

iedereen die het zou gebruiken, goede bedoelingen had en was te vertrouwen, dus SMTP controleert niet of je ook bent wie je zegt te zijn. De meeste SMTP servers gebruiken andere manieren om te bepalen of iemand is die hij/zij zegt te zijn, maar – in theorie – kan iedereen een willekeurige SMTP server gebruiker om e-mail te versturen. (voor meer informatie hierover, zie onderdeel **9.2.4 Vervalste Headers**.)
Het tweede dat je kunt opmerken is dat het geheime wachtwoord dat je verstuurt naar de POP server, in platte tekst wordt verstuurd. Misschien dat je op je scherm sterretjes ziet als je het intikt, maar als het wordt verstuurd, gebeurt dat in een vorm die gewoon leesbaar is. Iedereen die handig genoeg is om netwerkverkeer te bekijken – met een *packet sniffer* bijvoorbeeld – kan zo je wachtwoord zien. Misschien dat je denkt dat *jouw* netwerk veilig is, maar je hebt vermoedelijk weinig te zeggen over de andere netwerken waar je data over heen reist.
Het derde, en mogelijk belangrijkste dat je moet weten over e-mails, is dat ze – net als je wachtwoord – worden verstuurd en opgeslagen in platte tekst-formaat. Ze kunnen op elk moment, op elk deel van de route, worden bekeken.
Hieruit kun je maar 1 conclusie trekken: *e-mail is geen veilige manier om informatie te versturen*. Natuurlijk, het is handig om grappen uit te wisselen en een afspraak te maken voor een etentje of borrel, maar van alles wat je ook niet midden op een drukke straat rond zou bazuinen, zou je je af moeten vragen of je het dan wel in de e-mail wil zetten.
Klinkt dat paranoide? Ja, misschien is het dat wel, maar dat wil niet zeggen dat je niet voorzichtig genoeg kunt zijn. Veel van onze e-mails gaan over vrij onbelangrijke dingen. Weinig mensen anders dan jij, Sjonnie en Sjaan zullen willen weten dat je een diner-afspraak hebt op dinsdag. En zelfs als Truus wanhopig probeert te achterhalen waar jij, Sjonnie en Sjaan die dinsdag eten, dan is de kans klein dat ze met een packet sniffer probeert een netwerk af te tappen waarover je mailtjes reizen. Maar als bekend is dat een organisatie e-mail gebruikt bij het opzetten van credit card transacties, is het niet onwaarschijnlijk dat iemand zal proberen een manier te vinden om het netwerkverkeer af te luisteren en zo aan credit card gegevens te komen.

9.1.3 Web Mail

Een tweede optie voor e-mail is gebruik te maken van een web gebaseerd e-mail account. Daarbij gebruik je een webbrowser om je mail af te handelen. Omdat de e-mail voor zulke accounts normaal gesproken is opgeslagen op de web e-mail server – niet op je lokale computer – is het handig als je vanaf verschillende computers wil kunnen werken met je e-mail. Sommige ISP's maken het mogelijk je e-mail zowel via een lokale e-mail-client als via het web te gebruiken.
Sta er wel bij stil dat webpagina's op je lokale computer worden opgeslagen in de *cache*, soms voor behoorlijk lange tijd. Als je dus je e-mail afhandelt op de computer van iemand anders, kan het zijn dat je e-mails toegankelijk zijn voor andere personen die die computer gebruiken.
Web gebaseerde e-mail accounts zijn vaak gratis en makkelijk te verkrijgen. Daarmee heb je de mogelijkheid om meerdere online identiteiten aan te nemen. Zo kun je een e-mail-adres hebben voor communicatie met je vrienden, en een aparte voor communicatie met familie. Van zoiets kijkt niemand op, tenzij je je echt expres voordoet als geheel iemand anders.
Oefeningen:
1. Je kunt veel leren van hoe POP e-mail werkt en wordt opgehaald door gebruik te maken van het programma telnet. Als je telnet gebruikt in plaats van een e-mail client, moet je handmatig alle commando's tikken die je e-mail-client normaal gesproken 'onder water' automatisch uitvoert en uitwisselt met de mail-server. Gebruik een zoekmachine om op internet de instructies en commando's te vinden die nodig zijn om je e-mail

account te benaderen via het telnet programma. Wat zijn de nadelen van deze manier om je e-mail op te halen? Wat zijn mogelijke voordelen?
2. Vind drie organisatie die web gebaseerde e-mail services aanbieden. Welke beloftes maken ze, eventueel, op gebied van beveiliging die je via hen stuurt en ontvangt? Doen ze moeite om vast te stellen dat iemand die hun services gebruikt ook is die hij/zij zegt te zijn?
3. (mogelijk huiswerk) Bepaal welke SMTP server in gebruik is voor het email-adres dat je het meest gebruikt.

9.2 Veilig E-mail Gebruik Deel 1: Ontvangen

Iedereen gebruikt e-mail, en tot verassing van veel mensen kan je e-mail tegen je gebruikt worden. E-mail moet worden gezien als een postkaart: iedereen die kijkt kan zien wat er op/in staat. In een standaard e-mailtje zou je niets moeten zetten wat niet iedereen mag weten. Dat gezegd hebbende: er zijn manieren om je e-mail te beveiligen. In dit deel bespreken we veilig en verstandig e-mail-gebruik en hoe je je privacy online kunt beschermen.

9.2.1 Spam, Phishing en Fraude

Iedereen vindt het leuk om e-mail te ontvangen. Een hele tijd geleden, in een sterrestelsel ver, ver weg, kreeg je alleen mail van mensen die je kende, en het ging over dingen die je belangrijk vond. Tegenwoordig krijg je email van mensen waar je nog nooit van hebt gehoord die je software, drugs huizen en andere dingen proberen te verkopen, nog los van de mails van mensen die willen dat je ze helpt om 24 million Nigeria uit te krijgen. Dit type ongevraagde reclame-materiaal noemt men spam. Een hoop mensen kijken er van op dat een aan hen verstuurde mail de afzender nog meer gegevens over ze in handen kan geven, zoals het moment waarop de email werd geopend en hoe vaak de email was gelezen, of hij is doorgestuurd etc. Dit type technologie – met de naam web bugs – wordt gebruikt door zowel spammers als 'legale' afzenders. Ook het reageren op een e-mail of het klikken op een unsubscribe/opzeggen-link kan zorgen dat de afzender in ieder geval weet dat de mail bij een actief/'bemensd' e-mail-adres is afgeleverd. Een andere zorg voor privacy is de toename van "phishing" aanvallen. Heb je weleens een mail gehad waarin werd gevraagd om in te loggen bij je bank, e-bay of een andere site en je gegevens te controleren? Pas op met zulke mails, het kan een poging zijn om je inloggegevens te stelen. Om de kans te verkleinen dat je in zulke valstrikken trapt, kun je een aantal simpele maatregelen nemen; we behandelen ze hierna.

9.2.2 HTML E-Mail

Eén van de aandachtspunten (qua beveiliging) rond HTML e-mails is het gebruik van *web bugs*. Web bugs zijn onzichtbare afbeeldingen in je e-mail die een verbinding hebben met de webserver van de afzender en hem/haar een seintje geven dat jij de e-mail ontvangen of geopend hebt. Een andere zwakheid in HTML e-mail is dat de afzender links kan invoegen waarbij exact te zien is wie op welke link klikt.
Dit kan de afzender informatie geven over de status van het bericht. We adviseren daarom het gebruik van een e-mail client die je in staat stelt het automatisch laden van afbeeldingen uit te zetten. Een ander probleem ligt op gebied van scripts in de e-mail waarmee programma's geestart kunnen worden als je browser niet voorzien is van de laatste beveiligings-updates.
Veel web gebaseerde e-mail clients hebben de optie om het automatisch laden van afbeeldingen uit te zetten, of berichten te tonen in tekst-formaat. Beide opties zijn even slim, vanuit beveiligingsoogpunt. De beste manier om je zelf te beschermen tegen HTML e-mail gebaseerde beveiligings- en privacy-aanvallen is om een tekst-gebaseerde e-mail-client te gebruiken. Als je je e-mails echt in HTML-formaat 'moet' lezen, wees dan extra voorzichtig!

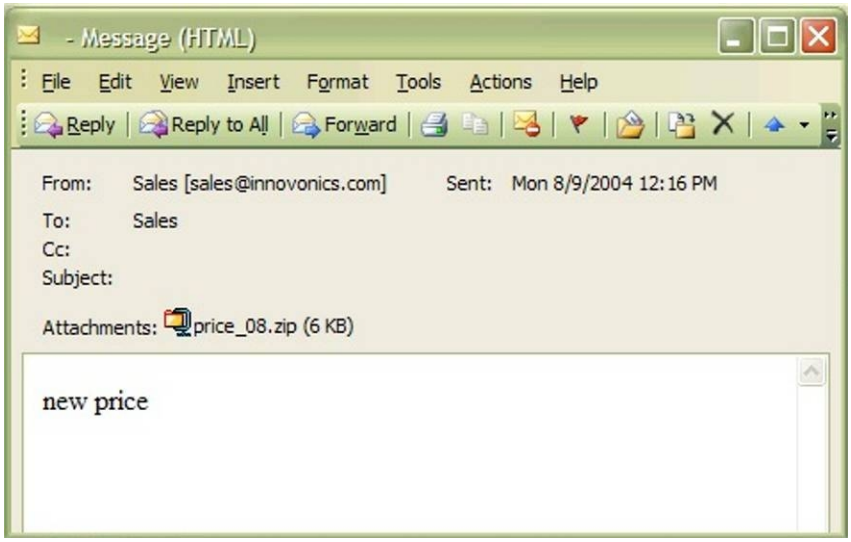
9.2.3 Beveiligingsaspecten van bijlages

Een andere zorg op gebied van ontvangen e-mails zijn bijlages. Aanvallers kunnen malware, virussen, Trojan horses en allerlei soorten vervelende programma's verzenden. De beste beveiliging is niets te openen van afzenders die je niet kent. Open zeker geen bestanden met

extensie .exe of .scr, omdat daarmee een programma wordt gestart waarmee je computer besmet kan worden met een virus. Goed gebruik is om elk toegestuurd bestand op te slaan op je lokale computer en te scannen met een antivirus-programma. Pas ook op met bestanden die er ongevaarlijk uit zien, zoals zip bestanden. Aanvallers kunnen uitvoerbare bestanden soms vermommen als een onschuldig bestand, door het icoontje te wijzigen, of de naam zo lang te maken en een dubbele extensie te gebruiken, zodat het bestand niet als risicovol uitvoerbaar bestand te herkennen is.

9.2.4 Vervalste headers

Je kunt ook e-mails ontvangen die afkomstig lijkt van iemand die je kent, of van betrouwbaar lijkende adressen als "Systeembeheer", "Administrator", "Postmaster" of "Security Team" van je ISP, school of werk. De onderwerp-regel kan iets zijn als
"Returned Mail" of "Hacking Activity" of andere woorden die zorgen dat je nieuwsgierig bent/wordt. Vaak zit er een bijlage bij, of een link om op te klikken. Het probleem is dat er geen technische kennis en ongeveer 10 seconden voor nodig is om een e-mail te sturen uit naam van een ander (afhankelijk van het land waar je leeft, kan dit *zeer* illegaal zijn).
Om dit te doen hoef je alleen maar wat instellingen in je e-mail-client te wijzigen. Op het scherm waar je gevraagd wordt wat je e-mail-adres is (b.v. onder *Opties*, *Instellingen* of *Voorkeuren*) tik je gewoon een ander e-mail-adres in. Vanaf dat moment zullen alle verstuurde e-mails een vals afzender-adres hebben. Betekent dat, dat niemand kan zien van wie de mail echt afkomstig is? Nee, niet echt. Iedereen die weet hoe hij/zij e-mail-headers moet bekijken en een huiszoekingsbevel kan bemachtigen, kan op basis van de informatie in die e-mail-header vermoedelijk achterhalen wie de echte afzender was/is. Dit alles betekent dat een spammer zich kan voordoen als een willekeurig ander. Dus als Fannie Gyotoku [telecommunicatecreatures@cox.net] je een magische antenne voor je mobiele telefoon probeert te verkopen, die bij aflevering een schoenendoos omwikkeld met zilverpapier blijkt te zijn,
kun je best gaan klagen bij cox.net, maar sta er niet van te kijken als ze je vertellen dat die gebruiker niet bij hen bekend is.
De meeste ISPs controleren of afzenders zijn wie ze zeggen te zijn en proberen te voorkomen dat mensen die niet bij hen bekend zijn, via hun SMTP server e-mail versturen. Het probleem is dat hackers en spammers vaak een SMTP server draaien op hun eigen PC, en zich dus niet hoeven te laten controleren door een ISP en het laten lijken zoals ze willen. Een manier om te bepalen of een verdacht uitziende mail problemen kan gaan opleveren, is de afzender te kennen en die op te bellen. Beantwoord nooit een e-mail waarvan je verdenkt dat hij vervalst is, omdat de afzender daardoor ziet dat hij 'beet' heeft (een e-mail-adres heeft bereikt waar iemand mee werkt). Je kunt ook naar de header-informatie kijken om te bepalen van waar de mail afkomstig is, zoals in onderstaand voorbeeld (om deze headerinformatie in Outlook2003 te bekijken, klik je naar view>options):




```
Microsoft Mail Internet Headers Version 2.0
Received: from srv1.mycompany.com ([192.168.10.53]) by mx1.mycompany.com
over TLS secured channel with Microsoft SMTPSVC(6.0.3790.0);
       Mon, 9 Aug 2004 11:20:18 -0700
Received: from [10.10.205.241] (helo=www.mycompany.com)
      by srv1.mycompany.com with esmtp (Exim 4.30)
      id 1BuEgL-0001OU-8a; Mon, 09 Aug 2004 11:15:37 -0700
Received: from kara.org (67.108.219.194.ptr.us.xo.net [67.108.219.194])
      by www.mycompany.com (8.12.10/8.12.10) with SMTP id i79IBYUr030082
      for <sales@mycompany.com>; Mon, 9 Aug 2004 11:11:34 -0700
Date: Mon, 09 Aug 2004 14:15:35 -0500
To: "Sales" <sales@mycompany.com>
From: "Sales" <sales@innovonics.com>
Subject:
Message-ID: <cdkdabgurdgefupfhnt@mycompany.com>
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="--------cfwriebwwbnnfkkmojga"
X-Scan-Signature: 178bfa9974a422508674b1924a9c2835
Return-Path: sales@innovonics.com
X-OriginalArrivalTime:     09     Aug     2004     18:20:18.0890     (UTC)
FILETIME=[868FEAA0:01C47E3D]
----------cfwriebwwbnnfkkmojga
Content-Type: text/html; charset="us-ascii"
Content-Transfer-Encoding: 7bit
```

```
----------cfwriebwwbnnfkkmojga
Content-Type: application/octet-stream; name="price_08.zip"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="price_08.zip"
----------cfwriebwwbnnfkkmojga—
```

Het deel waarin ik geinteresseerd ben, staat hierboven gemarkeerd. Merk op dat bij "Received" staat dat het bericht afkomstig is van kara.org op een IP-adres die lijkt te vallen onder een xo.net DSL lijn, en dat komt niet overeen met het in de mail zichtbare afzenders-domein innovonics.com.
Verder blijkt dat, als ik innovonics.coms mail server opzoek via nslookup, de adressen de volgende gegevens hebben:

```
C:\>nslookup innovonics.com
Server:  dc.mycompany.com
Address:  192.168.10.54

Non-authoritative answer:
Name:    innovonics.com
Address:  64.143.90.9
```

Dus ik was terecht op mijn hoede en de e-mail bevat vermoedelijk een soort malware in een uitvoerbaar bestand die zich voordoet als zip bestand. De malware heeft vermoedelijk de PC besmet van de persoon op de DSL lijn, waardoor die PC een zombie is geworden en kopieeen van de malware verstuurt naar iedereen in het adresboek van de besmette computer. Ik ben blij dat ik dit even heb uitgezocht!

Oefeningen:
1. (de Amerikaanse) Citbank en PayPal zijn de 2 meest populaire doelen voor phishing aanvallen via email. Zoek uit wat die 2 organisaties doen om phishing tegen te gaan. Kijk ook eens of je informatie kunt vinden over phishing bij je bank.
2. Zoek eens uit of je bank of credit-card-maatschappij een tekst online hebben over het gebruik van e-mail en je persoonlijke informatie.
3. (mogelijk huiswerk) Onderzoek eens een ontvangen spam-email and kijk of je kunt achterhalen wat de echte bron/afzender is.

9.3 Veilig E-mail Gebruik Deel 2: Versturen

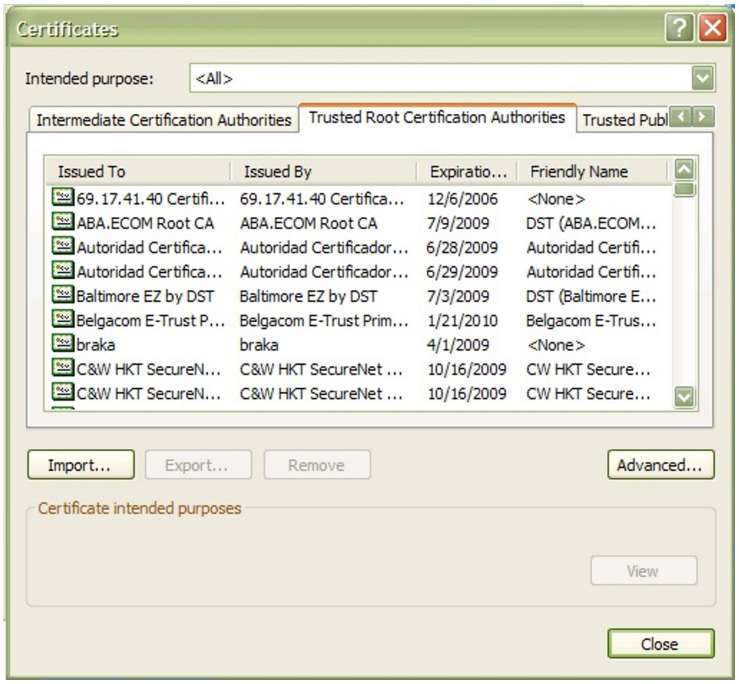
Zelf e-mails versturen is wat minder gevaarlijk. Je kunt echter een aantal dingen doen om je gesprek wat veiliger te maken. De eerste is te zorgen dat je verbinding veilig is (zie sectie **9.4 Beveiliging van de Verbinding** voor meer informatie). Er zijn ook mogelijkheden om je e-mails te voorzien van een digitale handtekening, zodat de ontvanger zeker weet dat het bericht van jou afkomstig is en niet is gewijzigd tijdens de verzending. En voor maximale beveiliging kun je je berichten vercijferen zodat niemand ze kan lezen.
Als je altijd een digitale handtekening gebruikt voor het versturen van belangrijke e-mail, dan heb je heel wat +-punten als er ooit iemand probeert zich als jou voor te doen. Je kunt ze ook gebruiken om e-mails te versleutelen zodat niemand anders dan de ontvanger ze kan lezen.

PGP stelt je in staat om je e-mails goed te beveiligen, en het breken van die beveiliging vergt extreem veel rekenkracht.

9.3.1 Digitale Certificaten

Een digitaal certificaat is uniek voor een individu, net zoals een rijbewijs of paspoort, en bestaat uit 2 delen. Het gaat om een publiek en privé deel. Het certificaat hoort bij één persoon, en ze worden verstrekt door een betrouwbare Certificate Authority, of CA. De lijst van Certificate Authorities die jij vertrouwt wordt automatisch verspreid (als je gebruiker bent van Microsoft
Windows) door Windows Update en de lijst is te benaderen in je browser, onder tools>internet options>content>certificates. Daar kun je zien welke certificaten er op je computer aanwezig zijn (je eigen certificaat en certificaten van anderen), en welke andere certificate authorities jij vertrouwt.

Je kunt er ook voor kiezen geen automatische updates van de CA's meer te ontvangen en je kunt ook alle CA's verwijderen uit de lijst, alhoewel dat niet wordt aangeraden. Instructies om dit te doen staat op de site van Microsoft.



9.3.2 Digitale Handtekeningen

Alle digitale handtekeningen worden gegenereerd door je e-mail software in combinatie met je privé sleutel, zodat ontvangers zeker kunnen zijn dat de mails van jou afkomstig zijn. De handtekening heeft 2 doelen. Het eerste is dat men zeker weet dat de email door jou verstuurd is. Dit heet ook wel non-repudiation (onweerlegbaarheid). Het tweede is om zeker te stellen dat de inhoud niet is gewijzigd. Dat heet data integrity (integriteit). De manier waarop dat bereikt wordt is dat je bericht door een "one way hash"-functie wordt bewerkt.

Daamee wordt een waarde bepaald, de "message digest". Dit is een unieke waarde, en als de toegepastte formule 'sterk' is, heeft de message digest de volgende kenmerken:
 Het originele bericht kan niet worden gereproduceerd uit de digest.
 Elke digest is uniek.
Nadat de digest is aangemaakt, wordt hij versleuteld met je privé sleutel. De versleutelde digest wordt toegevoegd aan je originele e-mail, samen met het publieke deel van je sleutel. De ontvanger opent vervolgens het bericht, en de digest wordt ontcijferd met je publieke sleutel. De digest wordt vergeleken met een identieke digest die wordt gemaakt door het mail-programma van de ontvanger. Als ze overeenkomen, ben je klaar.
Zo niet, dan laat je e-mail-programma je weten dat het bericht is gewijzigd. Er zijn 2 vormen van ondertekening / versleuteling, S/MIME en PGP. S/MIME wordt gezien als de oplossing voor grote bedrijven en de overheid, mogelijk omdat er gebruik wordt gemaakt van de minder arbeidsintensieve certificate authority manier van authenticatie, en omdat het makkelijker te gebruiken is in combinatie met Microsoft's Outlook Express e-mail programma. PGP wordt vaker gebruikt binnen de gemeenschap van computer-specialisten, omdat er voor de authenticatie gebruik wordt gemaakt van een decentraal *web of trust* model, waar de betrouwbaarheid van een gebruiker wordt gecontroleerd via het "vriend van een vriend"-systeem, waarbij geldt dat als jij mij vertrouwt, je ook de mensen die ik vertrouw, kunt vertrouwen; en omdat mensen die handig zijn met computers het geen probleem vinden om 4 uur bezig te zijn om Thunderbird aan de praat te krijgen in combinatie met PGP

– dat soort uitdagingen is voor een een vorm van *ontspanning*.

9.3.3 Een certificate bemachtigen

Als je een digitaal certificaat of digitaal ID wil bemachtigen, moet je contact opnemen met een
Certificate Authority (Verisign en Thawte zijn de bekendste, maar als je zoekt op het internet vind je er vast nog meer.) Bij beide moet je jezelf identificeren om te bewijzen dat je bent wie je zegt te zijn. Bij Thawte kun je een gratis certificaat krijgen, maar zij vragen wel een hoop persoonlijke gegevens, waaronder je Sofi-nummer. Verisign brengt kosten in rekening voor een certificaat, en die moet je betalen met een credit card, maar ze vragen niet zoveel persoonlijke informatie. (Eigenlijk gaat Verisign er van uit dat de credit card maatschappij je persoonlijke gegevens heeft gecontroleerd.) Misschien voel je je wat ongemakkelijk om dit soort bedrijven persoonlijke informatie te verstrekken, maar bedenk wel dat zij garant staan dat jij zegt te zien wie je bent en te vertrouwen bent. Vraag – zoals altijd – bij je ouders of opvoeders na of het o.k. is om persoonlijke informatie te verstrekken op een website (zeker als je hun credit-card gebruikt en kosten gaat maken).
Het grootste nadeel van het gebruik van een certificate authority is dat je privé sleutel in handen is van iemand anders – de certificate authority. Als er wordt ingebroken bij de certificate authority is je digitale ID in gevaar.

9.3.4 Encryptie

Als extra beveiligingslaag kun je je e-mails versleutelen (*encrypten*). Versleuteling zorgt er voor dat je e-mail-tekst wordt omgezet naar een chaos van cijfers en letters, en alleen leesbaar gemaakt kan worden door de geadresseerde. Je diepste geheimen en slechste gedichten zullen onleesbaar zijn, behalve voor de mensen die je echt vertrouwt.
Bedenk echter dat, alhoewel dit waarschijnlijk geweldig in je oren klinkt – en bij iedereen die niet zonodig slechte gedichten wil lezen – niet alle overheden dit goedkeuren. Hun argumenten zullen – wel of niet – redelijk zijn (daar kun je het eens met anderen over hebben), maar daar gaat het hier niet om. Punt is dat, afhankelijk van de wetgeving in een

land, het versleutelen van je berichten een overtreding/misdaag kan zijn, los van de inhoud van het bericht.

9.3.5 Hoe werkt het?

Encryptie is nogal gecompliceerd, dus we leggen het hier zo simpel mogelijk uit:
Jan wil een versleuteld bericht versturen. Het eerste wat Jan doet is een Certificate Authority bezoeken en een Digitaal Certificaat aanvragen. Dit Certificaat bestaat uit 2 delen, een publieke sleutel en een privé sleutel.
Als Jan versleutelde berichten wil ontvangen en versturen met zijn vriendin Karin, zullen ze eerst hun publieke sleutel moeten uitwisselen. Als je een sleutel ophaalt bij een Certificate Authority die je vertrouwt, kun je automatisch laten controleren of de sleutel geldig is. Dat betekent dat je e-mail programma controleert of het certificaat geldig is, en nog niet is ingetrokken (revoked).
Als het certificaat niet afkomstig is van een authority die je vertrouwt, of wanneer het gaat om een PGP sleutel, dan moet je de vingerafdruk van de sleutel controleren. Normaal gesproken wissel je daarbij in real life (IRL, face-to-face) de sleutel of de vingerafdruk-gegevens uit.
We nemen nu aan dat Jan en Karin vergelijkbare encryptie-schema's gebruiken, en ze versleutelde berichten hebben uitgewisseld zodat ze elkaars publieke sleutel hebben.

Als Jan een versleuteld bericht wil versturen, wordt zijn bericht-tekst eerst versleuteld naar een pre-hash-code. Die code wordt gegenereerd met een wiskundige formule, het encryptie-algoritme. Er zijn veel soorten algoritmes, maar voor e-mail worden voornamelijk S/MIME en PGP gebruikt.
De hash code van Jan's bericht is versleuteld door het e-mail programma met behulp van de privé -sleutel van Jan. Jan gebruikt dan de publieke sleutel van Karin om het bericht te versleutelen, zodat alleen Kira het weer kan ontcijferen met haar privé-sleutel, daarmee is het hele encryptie-proces doorlopen.

9.3.6 Ontcijferen

Dus Karin heeft een versleuteld bericht ontvangen van Jan. Dat is meestal te zien omdat er dan een sleutel te zien is in haar inbox. Het ontcijferen van een bericht wordt afgehandeld door haar e-mail programma, maar achter de schermen gebeurt globaal het volgende:
Karin's e-mail programma gebruikt haar privé-sleutel om de pre-hash code en het bericht te ontcijferen.
Dan vraagt Karin's e-mail programma de publieke sleutel van Jan op uit haar sleutel-verzameling (want we hebben eerder sleutels uitgewisseld). Die publieke sleutel wordt gebruikt om de pre-hash-code te ontcijferen en vast te stellen dat het bericht van Jan afkomstig is. Karin's e-mail programma genereert vervolgens een post hash code op basis van het bericht. Als de post hash code gelijk is aan de pre hash code, dan is het bericht niet gewijzigd tijdens de verzending.
Opmerking: als je je privé-sleutel kwijt raakt, zijn al je vercijferde berichten waardeloos geworden, dus je moet iets bedenken om een backup te maken van je privé- en publieke sleutel.

9.3.7 Is Encryptie te breken?

Als je naar de cijfers kijkt, is de versleuteling die die PGP biedt, niet te kraken. Natuurlijk, als je een miljoen computers tot je beschikking hebt en kunt laten stampen dan lukt het uiteindelijk

wel, maar pas als die miljoen apen het verhaal van Romeo en Juliet af hebben. De getal-theorie die de basis is van de versleuteling ligt in gebruik van enorme priemgetallen, en, ondanks het feit dat veel wiskundigen priemgetallen uitvoerig hebben bestudeerd, is er nog geen manier gevonden om deze methode makkelijk te kraken.
Maar versleuteling en privacy gaat over meer dan alleen cijfers. Als iemand je privé-sleutel weet te bemachtigen, heeft hij toegang tot al je vercijferde spullen. Versleuteling is dus maar een onderdeel van een complex van beveiligings-maatregelen waarmee wordt gezorgd dat je privé-sleutel en je wachtwoord(zinnen) (pass-phrase) bescherm worden.

Oefeningen:

1. Is encryptie van email legaal in het land waar je woont? Zoek (nog) een land waarin het legaal is, en zoek een land waarin het (ook) illegaal is.
2. Science fictie-schrijvers hebben twee soorten werelden bedacht, één waarin de levens van mensen geheel transparant zijn en niemand dus geheimen heeft, en één waarin ieders gedachtes en communicatie helemaal privé is. Phil Zimmerman, maker van PGP, gelooft in privacy als bron van vrijheid. Lees zijn gedachtes over waarom je PGP nodig hebt op http://www.pgpi.org/doc/whypgp/nl/ . Bekijk vervolgens het artikel van science fiction schrijver David Brin's 'A Parable about Openness' op http://www.davidbrin.com/akademos.html waarin hij een aantal voordelen noemt van openheid als bron van vrijheid. Bespreek die twee tegenstrijdige zienswijzes eens. Welke spreekt jou het meeste aan? Welke werkt volgens jou het best 'in de echte wereld'/de praktijk? Wat denk jij dat de toekomst van de privacy is?

9.4 Beveiliging van de Verbinding

Tot slot is er nog de beveiliging van de verbinding. Webmail moet je alleen gebruiken over een SSL-verbinding. In de onderste regel van de browser zie je dan een klein slot-symbooltje. Als je POP and en een e-mail client gebruikt, zorg dan dat je email client hebt ingesteld dat SSL met POP over poort 995 en SMTP over poort 465 moet worden gebruikt. Daarmee wordt je e-mail versleuteld op de route tussen jou en de server, terwijl ook je POP / SMTP gebruikersnaam en wachtwoord wordt beschermd. Je ISP zou een “Hoe kan ik” op hun website moeten hebben over hoe je dit instelt. Als ze geen veilige POP / SMTP verbinding aanbieden, verander dan van ISP!

Oefening:

Als je een e-mail account hebt, zoek dan uit of je account voor de verbinding gebruik maakt van SSL. Hoe controleer je dat in je e-mail client? Heeft je ISP informatie over het gebruik van een SSL-verbinding?

Meer lezen?

Can someone else read my e-mail?
http://www.research.att.com/~smb/securemail.html
MIT's PGP freeware page
http://web.mit.edu/network/pgp.html
General news on Internet privacy issues:
Electronic Privacy Information Center
http://www.epic.org/
and
Electronic Frontier Foundation
http://www.eff.org/
More about PGP
http://www.openpgp.org/index.shtml
How Reading an Email Can Compromise Your Privacy
http://email.about.com/od/staysecureandprivate/a/webbug_privacy.htm
Avoiding E-mail Viruses
http://www.ethanwiner.com/virus.html
A Brief Overview of E-mail Security Questions (with a short advertisement at the end)
http://www.zzee.com/email-security/
A Brief Overview of E-mail Security Questions (with no advertisement)
http://www.claymania.com/safe-hex.html
Windows Based E-mail Precautions
http://www.windowsecurity.com/articles/Protecting_Email_Viruses_Malware.html
http://computer-techs.home.att.net/email_safety.htm
Differences Between Linux and Windows Viruses (with information on why most Linux e-mail programs are more secure)
http://www.theregister.co.uk/2003/10/06/linux_vs_windows_viruses/