Frank Brokken / f.b.brokken@rug.nl

Certificaten

Frank Brokken is security manager bij het CIT. Met het instellen van deze functie probeert de RUG het 'security bewustzijn' bij de gebruikers van de universitaire ICT-voorzieningen te bevorderen. In zijn column houdt Frank ons op de hoogte van de stand van zaken met betrekking tot zijn missie.

In het voorjaar schreef ik in Pictogram over de mogelijkheid om e-mail te authenticeren en te versleutelen met behulp van certificaten. Onlangs bleek weer eens dat dit geen overbodige luxe is.

Krom Nederlands

Eind september werd de RUG overspoeld met een nieuwe 'phishing'-poging waarin RUG-medewerkers in dreigende bewoordingen werden gemaand om username en password even op te sturen. De tekst van die phishing-poging luidde als volgt:

Date: Thu, 30 Sep 2010 17:44:29 +0700
From: University of Groningen <upgrad@webmaster.com>
Reply-to: upgrading@info.al
To: undisclosed-recipients:;
Subject: Geachte Rijksuniversiteit Groningen Internet-gebruiker

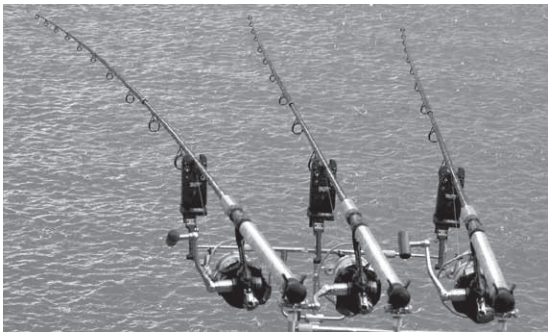
Geachte Rijksuniversiteit Groningen Internet-gebruiker,

Om uw account Verificatie proces, bent u op dit bericht antwoord en uw ID en wachtwoord in te voeren in de daarvoor bestemde ruimte (********), bent u verplicht om dit te doen voor de volgende 48 uur na ontvangst van deze e-mail, of uw webmail account wordt gedeactiveerd en gewist uit onze database.

Volledige naam:
Webmail User ID:
webmail Wachtwoord:

Uw account kan ook worden gecontroleerd op https: / / mailbox.rug.nl / Dank u voor het gebruik van www.rug.nl Support Copyright 2008 Rijksuniversiteit Groningen Internet Support.

Je blijft natuurlijk lachen om dit soort pogingen die direct opvallen door het kromme Nederlands, maar ook de vissers leren de taal en langzaamaan wordt het Nederlands in hun teksten steeds beter.

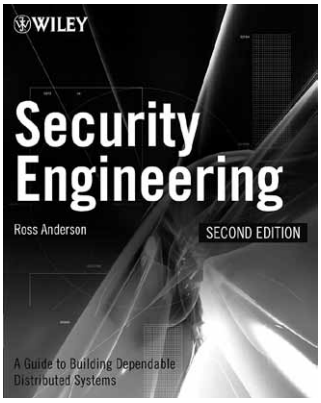


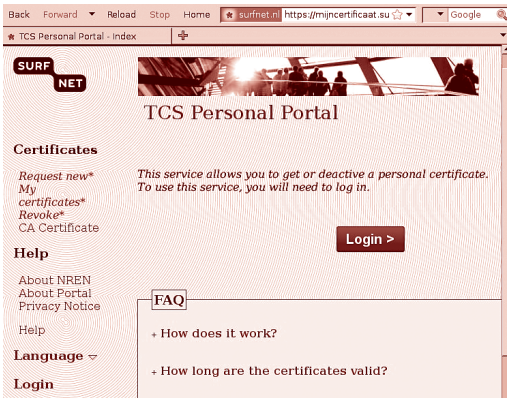
Dat dit op termijn goed fout kan gaan en dat overheden van diverse landen het slachtoffer van vissers kunnen worden, leert onder andere de website Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network: **www.scribd.com/doc/13731776/**. Wie geïnteresseerd is in het door Scribd gepubliceerde rapport: het kan (ook) bij mij worden opgevraagd. Andere voorbeelden van overheden die belaagd worden door vissers, is te vinden op de website **www.wired.com/threatlevel/2009/03/spy-system-focu/**.

Haas met sterretjes

Voor zover bekend is niemand binnen de RUG in de valkuil van boven vermelde vispoging getrapt. Kudos, beste collega's! Het mooiste vond ik nog de reactie van iemand die mij schreef dat zijn (gebruikers-) naam 'Haas' was en zijn password uit acht sterretjes bestond. Minder complimenteuze gebruikersnamen en wachtwoorden zijn mij naar aanleiding van deze vispoging ook medegedeeld. Boeiend hoor, zo'n Security Manager-functie!

Maar wat kunnen we nou ondernemen om in





de toekomst niet in een of ander visvijvertje te vallen? Het antwoord zal duidelijk zijn: alleen reageren op fatsoenlijk geauthentiseerde e-mail.

Mogelijk dat ik zelf op termijn alleen nog maar op geauthenticeerde e-mail (zeker van collega's) zal reageren, omdat het inmiddels voor iedereen mogelijk is om op eenvoudige wijze zijn/haar e-mail te authenticeren. Daarbij wordt gebruik gemaakt van zogenaamde S/MIME-certificaten die alle medewerkers van de RUG inmiddels zonder kosten kunnen aanvragen op basis van een overeenkomst tussen Comodo, Terena en SURFnet.

S/MIME staat voor 'Secure Multipurpose Internet Mail Extensions' en met zo'n certificaat kun je aan iedereen die het Comodo-basiscertificaat (zo'n ding heet eigenlijk 'certificate authority root certificate') in zijn/haar mailprogramma heeft opgenomen duidelijk maken dat de gestuurde e-mail inderdaad van u, en niet van een visser, afkomstig is. Overigens is het Comodo-basiscertificaat standaard in het mailprogramma opgenomen. Die hobbel is dus alvast genomen.

OK. Voor het geval er nog steeds lieden zijn die denken dat het zo'n vaart niet loopt: lees toch vooral eens het Scribd-rapport en neem eens de moeite om het eerste hoofdstuk van Ross Anderson's 'Security Engineering' te lezen.

Elektronische handtekening

Voor wie geregistreerd staat als personeelslid van de RUG is het uitermate simpel om een S/MIME-certificaat te krijgen. Ook wie geen RUG-medewerker is, maar bijvoorbeeld wel tot een SURFnet-doelgroep behoort (bijvoorbeeld UMCG of Hanzehogeschool Groningen) komt zeer waarschijnlijk eveneens in aanmerking voor zo'n certificaat: neem desgewenst contact op met uw SURFnet-contactpersoon of rechtstreeks met SURFnet voor nadere informatie.

RUG-medewerkers kunnen een certificaat aanvragen op **https://mijncertificaat.surfnet.nl/**. Merk op dat dit zelf een met een certificaat gevalideerde website is: controleer het bijbehorende certificaat (dat is altijd een goed idee bij https-verbindingen). In dit geval is het certificaat uitgegeven op naam van SURFnet (en zo hoort dat ook: website- en certificaatnamen moeten corresponderen) door Terena, die uiteindelijk is gevalideerd door Comodo zelf.

Na het inloggen (met het RUG P-nummer en bijbehorende password) kan een certificaat worden aangevraagd door de 'Request New'-link te volgen. De aanvraag zelf verloopt in een paar stappen, waarvan het behandelen hier te veel ruimte zou vergen. Een uitgebreide toelichting op de aanvraagprocedure vindt u echter onder **www.rug.nl/cit/security/adviezen/email**.

De aanvraagprocedure zelf resulteert in de ontvangst van een gesigneerd S/MIME-certificaat, en in een privécertificaat dat kan worden gebruikt om e-mail te voorzien van een 'elektronische handtekening' waarmee u uw e-mail kunt authenticeren.

Wachtzin

Niemand anders dan de eigenaar van het privécertificaat kan de elektronische handtekening plaatsen. Daardoor kan de ontvanger van uw e-mail verifiëren dat u (en niet een visser namens u) de e-mail heeft gestuurd.

Als extra beveiliging is uw privécertificaat voorzien van een 'wachtzin': een zin in plaats van een wachtwoord. Als eigenaar van uw S/MIME-certificaat weet u wat uw wachtzin is en uw mailprogramma kan uw e-mail voorzien van uw elektronische handtekening nadat u uw wachtzin heeft ingetypt.

Uiteindelijk wordt uw elektronische handtekening geverifieerd door uw certificaat waarvan de echtheid door Comodo is gegarandeerd. Dat hele proces verloopt automatisch, en het enige dat u in de praktijk nog hoeft te doen om de authenticiteit van uw e-mail te bewaken, is uw wachtzin in te typen.

Vertrouwelijke informatie kan eveneens veilig per e-mail worden verstuurd door gebruik te maken van de mogelijkheden die S/MIME biedt om informatie te 'versleutelen'. Door gebruik te maken van versleuteling kunt u bewerkstelligen dat alleen u (als afzender) en de geadresseerde (als ontvanger) toegang kan krijgen tot de vertrouwelijke informatie. Hoe dat moet, wordt eveneens uitgelegd op **www.rug.nl/cit/security/adviezen/email**.

Fatsoenlijke authenticatie

De mogelijkheden die door S/MIME-certificaten worden geboden, worden ook door PGP/GPG (Pretty Good Privacy/Gnu's Privacy Guard) geboden. PGP/GPG wordt standaard al binnen de RUG in Thunderbird ondersteund. Het essentiële verschil tussen PGP/GPG en S/MIME is dat bij PGP/GPG de gebruikers ervan elkaar moeten hebben ontmoet om de authenticiteit van hun PGP-certificaten (in deze context 'public keys' genoemd) te verifiëren. Bij S/MIME wordt de relatie tussen S/MIME-certificaat en de eigenaar door de certificaatautoriteit (Comodo, in ons geval) geverifieerd. Je zou kunnen zeggen dat daarom S/MIME iets eenvoudiger is te gebruiken dan PGP/GPG.

Maar waar het uiteindelijk om gaat, is dat we onze e-mail fatsoenlijk kunnen authenticeren, onder andere om op deze manier 'phishing'-pogingen verder te bemoeilijken.

Frank B. Brokken,
(Authentiek versleutelaar)