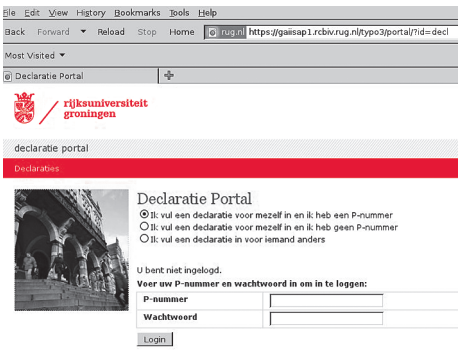
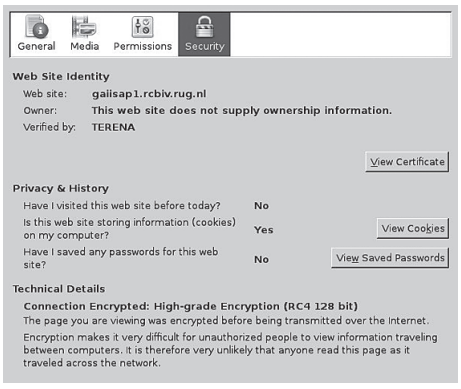
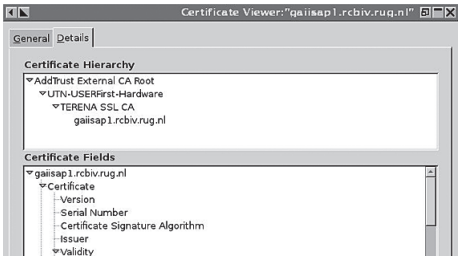
Frank Brokken / f.b.brokken@rug.nl

Het beveiligen van beveiligers

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.







Onlangs spraken collega's ons aan over de status van de certificaten zoals die worden gebruikt om bijvoorbeeld veilig in te loggen op de RUG-website. De toegang tot alle RUG-webapplicaties waarbij authenticatie (p-nummer/username en password) vereist zijn (zoals de declaratieportal), worden beveiligd met certificaten. Hierdoor kunnen wij als gebruiker onder andere verifiëren dat we geen contact hebben met een 'phishing' site, waar wordt geprobeerd ons onze authenticatiegegevens afhandig te maken.

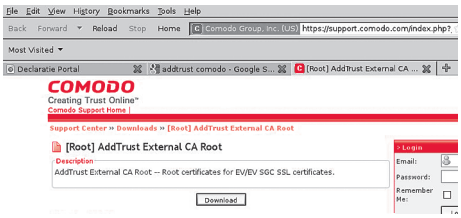
Interessante informatie

Een dergelijk certificaat kun je gemakkelijk opvragen door op het blauwe 'rug.nl'-venstertje in de adresbalk te klikken. Je krijgt dan te zien dat er een verbinding is met 'rug.nl', geverifieerd door TERENA. Ook is er de mogelijkheid om meer informatie op te vragen. Doe je dat, dan verschijnt er onder andere informatie over de aard van de beveiliging en de gebruiksgeschiedenis.

Maar de echt interessante informatie krijg je te zien wanneer de optie 'View Certificate' wordt geselecteerd, en dan het tabblad 'Details' wordt gekozen.

Rara

Voor dit Pictogram-verhaal is het bovenste deel van het tabblad 'Details' van belang: de 'Certificate Hierarchy'. Wat we hier zien, is dat het certificaat voor 'gaiisapl.rcbiv.rug.nl' is uitgegeven door TERENA, dat TERENA's certificaat



is uitgegeven door UTN-USERFirst-Hardware, en dat UTN-USERFirst-Hardware's certificaat is uitgegeven door AddTrust, dat een 'External CA Root' is.

Rara, wie of wat is AddTrust? Om te beginnen is het een CA, oftewel Certificate Authority. AddTrust vormt het begin van de 'Certificate Hierarchy' waarvoor Comodo, de feitelijke CA, verantwoordelijk is.

De vraag die ons door collega's is gesteld, heeft direct te maken met Comodo, omdat men vreesde, een vrees die onder andere is aangewakkerd door een artikel in een eerdere Pictogram (nr. 2, 2011), dat de Comodo-certificaten niet (meer) te vertrouwen zouden zijn.

De klok en de klepel

De achtergronden van het gebruik van certificaten is nog niet zo simpel, en het is eenvoudig om het spoor bijster te raken: men heeft de klok horen luiden maar weet eigenlijk niet zo goed waar de klepel hangt.

Nou, die klepel hangt prima, hoor. Wie een officiele CA wil zijn, moet aan een waslijst van strenge eisen voldoen, en controle daarop wordt zeer

regelmatig door daartoe gemachtigde auditors uitgevoerd. Inbreken bij Comodo is tot daar aan toe, maar dan ben je nog niet - als inbreker - waar je waarschijnlijk zijn wilt.

Een passage als 'Comodo is gehackt' is dan ook laten we zeggen - tendentieus. Het suggereert iets wat simpelweg niet waar is. Om een analogie van onze collega Adri Mathlener te gebruiken: 'Als je inbreekt bij de Nederlandse bank, heb je weliswaar ingebroken, maar heb je nog geen toegang tot de kluis'. Dat geldt ook voor het inbreken bij Comodo: 'hacken' is misschien mogelijk, maar dan ben je nog niet bij het 'AddTrust CA root certificate'. Daar kom je namelijk niet bij, om fysieke redenen...

Wat er wel is gebeurd

Op 15 maart jl. slaagt een hacker erin om toegang te krijgen tot een certificaat 'reseller'. Zo'n reseller kan worden vergeleken met een onderaannemer. De reseller kan certificaten uitgeven voor een subdomein. Wij zijn, samen met onze CIT-collega Anke Breeuwsma, reseller voor de RUG; TERENA is dat voor ons; UTN-USERFirst is dat voor TERENA; en UTN-USERFirst is dat voor Comodo. De hacker kreeg toegang tot de onversleutelde passwords van een aantal klanten van zo'n reseller. Van wie ook weer? Hier zijn er een paar (in totaal waren het er negen), sommige zullen bekend klinken:

login.live.com
mail.google.com
www.google.com
login.yahoo.com
login.skype.com
addons.mozilla.org
"Global Trustee"

Deze klanten konden certificaten maken en deze via de reseller laten signeren. Maar omdat de hacker toegang had tot de authenticatiegegevens konden valse certificaten in omloop worden gebracht. We herstellen bij dezen de misvatting dat Comodo zou zijn gehackt. Niet Comodo, maar een reseller was gehackt. Jammer dan: die had z'n zaakjes niet goed op orde. Moet ie ook niet zo dom zijn om passwords onversleuteld op te slaan.

Maar valse certificaten zijn potentieel ernstig. Doen genoemde domeinen niet denken aan 'cloud computing'? Oeps...

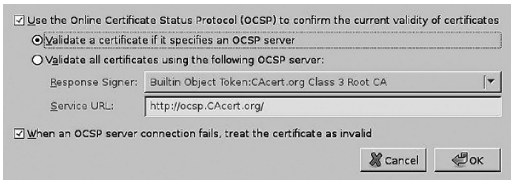
Misvatting

Om nog een voorbeeld te geven: wie valse RUG-certificaten in omloop brengt, kan de indruk wekken een RUG-site te zijn, en op die manier bijvoorbeeld login-gegevens van medewerkers en studenten achterhalen. Of, de zaak nog iets escalerend: wie valse bankcertificaten in omloop brengt, kan login-gegevens en tan-codes van banken verzamelen en misbruiken.

Slecht nieuws dus, zou je zo zeggen. Maar alleen wanneer je gebruik maakt van de tak waaronder jouw organisatie hangt. De reseller die z'n zaakjes niet op orde had was 'Global Trust', gevestigd in Italië. Slechts de beveiliging van verbindingen met domeinen die onder hun autoriteit vallen, wordt door het misbruik getroffen. We herstellen bij dezen de misvatting dat Comodo-certificaten, bijvoorbeeld die welke bij de RUG worden gebruikt, niet meer te vertrouwen zouden zijn.

Loftrompet

Op 20 maart startte een discussie bij Mozilla over de vraag of Comodo resellers nog wel te vertrouwen zijn en of - bij implicatie - Comodo zelf er wel goed aan doet om resellers zelf certificaten te laten signeren. Maar Comodo, ook niet gek, herroept onmiddellijk de uitgegeven certificaten. Mozilla reageert prompt met het steken van de loftrompet over Comodo's snelle en adequate reactie. Hoe gek zijn wij eigenlijk? Weten wij wel of de certificaten die we gebruiken wellicht te herroepen zijn? Dat is eenvoudig



te doen: In Firefox/Iceweasel open via 'Edit' het 'Preferences' window. Klik dan op 'Validation' en controleer of de vinkjes staan zoals in de weergegeven afbeelding.

Lekker veilig allemaal

De instellingen in de weergegeven afbeelding betekenen dat alle certificaten worden geverifieerd en dat ze alleen worden geaccepteerd als hun validiteit is bevestigd. Comodo, nog steeds niet gek, voert per direct een extra controlemaatregel in: alle certificaten die via Comodo worden uitgegeven, moeten met de hand worden gecontroleerd. Dat is voor ons niks nieuws. Dat doen wij altijd al, en hetzelfde geldt voor de TERENA-certificaten. Maar de gecompromitteerde reseller deed dat niet, en liet automatische uitgave toe. Dat is natuurlijk ook niet zo slim.

Kortom, om een kopje uit de eerdere Pictogram hier maar eens te herhalen: het is nog steeds 'lekker veilig allemaal'. Nou ja, voor wie zich realiseert dat een beveiligde verbinding slechts een 'conditio sine qua non' is. Misbruik kan ook dichter bij huis optreden, bijvoorbeeld doordat er zich 'malware', kwaadwillende software, in uw browser heeft genesteld. Nou ***dat*** is pas lachen! En de sleutel van die schatkist? Nou die is nog steeds waar die hoort, en niet bij de hacker. Reken maar!

Hopko Meijering,
Frank Brokken
(schatbewaarders en klokkenluiders)