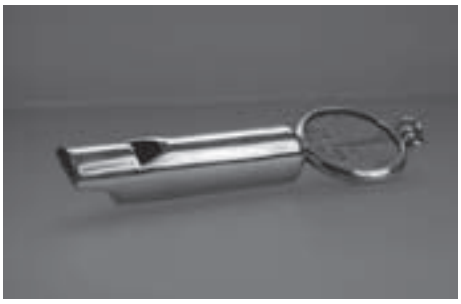
Frank Brokken / f.b.brokken@rug.nl

Preventief Onderhoud

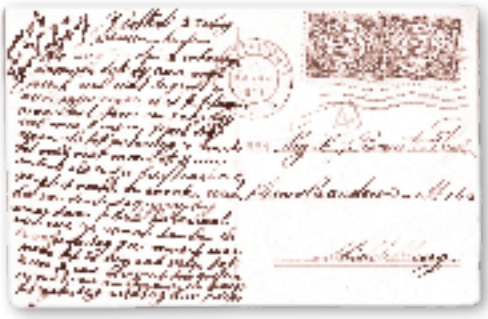
Frank Brokken is security manager bij het CIT. Met het instellen van deze functie probeert de RUG het 'security bewustzijn' bij de gebruikers van de universitaire ICT-voorzieningen te bevorderen. In zijn column houdt Frank ons op de hoogte van de stand van zaken met betrekking tot zijn missie.

Elk jaar moet mijn ouwe, trouwe bestelbus naar de garage voor de APK-keuring. Meteen ook een goed moment voor een onderhoudsbeurt. En elk jaar staat er op de rekening van de garage een post voor een nieuw oliefilter.

Was dat filter dan niet meer goed? Nee, het filter was prima, maar je auto kan nou eenmaal niet zonder zo'n ding en om te voorkomen dat je in de problemen komt door een verouderd filter, wordt het filter vervangen bij onderhoudsbeurten. Voorkomen is beter dan genezen, is het devies van preventief onderhoud.



Ansichtkaart uit 1920



Preventief onderhoud is niet iets wat je alleen maar bij auto's en andere machines tegenkomt, hoewel het daar wel het duidelijkst zichtbaar is. Preventief onderhoud is een wereld op zich. Er zijn boeken over geschreven en er zijn tijdschriften die zich daar louter en alleen op richten.

In deze Pictogram-bijdrage richt ik mij deze keer op preventief onderhoud van een encryptie-software. Het afgelopen jaar heeft de CIT-afdeling Opleidingen herhaaldelijk cursussen in het gebruik van persoonlijke encryptie (PGP/GPG) georganiseerd, en heeft Mark Meinema in een brede presentatie laten zien hoe makkelijk het is om e-mail namens iemand anders te sturen. Gelukkig is de remedie (het gebruik van encryptie om integriteit en authenticiteit van e-mail en andere informatie te garanderen) ook eenvoudig. E-mail sturen is als het verzenden van een ansichtkaart (de kaart is in 1920 gepost) en dus ook net zo (of beter) leesbaar.

Inmiddels leven we niet meer in de vorige eeuw (hooguit mentaal...) en is het inmiddels een fluitje van een cent om e-mail authenticatie en encryptie te gebruiken waar dat nodig is.

Unieke reeks

Maar de tijd gaat voort en daarmee ook onze rekenkracht. Deze verdubbelt ongeveer elke twee jaar en vroeg of laat is een encryptiemethode van gisteren morgen verouderd.

Zo ver is het nog niet, maar het zit in de pijplijn. Wat al wel gebeurt, is het volgende: wanneer je een e-mailbericht signeert (zodat de afzender door de ontvanger kan worden geauthenticeerd) wordt er een berekening op de te versturen e-mail uitgevoerd die tot een reeks tekens leidt die uniek is voor de desbetreffende e-mail. Elke letter die in de mail wordt gewijzigd, leidt tot een dramatische verandering van die reeks. Bijvoorbeeld: wanneer ik zo'n berekening op dit verhaal uitvoer (tot en met deze komma), dan krijg ik:
b510d2a1928c7780340459d824dff9c898675407

Wanneer ik nou de komma in een punt verander dan wordt de reeks:
878e9d7c61f00f821df90fb4b1deacc4b6b73753

Het is vervolgens deze reeks die met je elektronische handtekening wordt gesigneerd. Dat is

minder werk dan een heel document signeren en net zo veilig.

Tenminste... wanneer ik niet een ander document kan maken dat dezelfde reeks oplevert. Want in dat geval zou iemand het oorspronkelijke document ongemerkt kunnen vervangen door het alternatieve document.

Die situatie doet zich niet voor, maar zou zich met de gebruikelijke berekeningsmethode op afzienbare termijn kunnen gaan voordoen. Om die reden is er enig preventief onderhoud nodig aan de op dit moment gebruikte PGP-sleutels en PGP-instellingen. Over dat onderhoud gaat het vervolg.

Aanpassen PGP-instellingen

Om te beginnen moeten de instellingen van PGP worden aangepast. Dat moet via de *command-line* worden uitgevoerd. Het gaat als volgt:

1 Open een command-window (**Start** -> **Run**, vul in 'cmd' (zonder de quotes) en druk op **Enter**).
Ga naar je gpg directory.
Als je niet weet waar dat is geef dan de opdracht gpg --version
De tweede paragraaf van de uitvoer begint met de tekst 'Home:' waarachter de locatie van je GPG directory staat.
Ga naar die directory.

2 In die directory staat een file 'options' of 'gpg.conf'
Voeg aan die file (gebruik bijvoorbeeld Notepad) de volgende regels toe:
personal-digest-preferences SHA256
cert-digest-algo SHA256
default-preference-list SHA512 SHA384 SHA256 SHA224 AES256 AES192 AES CAST5 ZLIB BZIP2 ZIP Uncompressed
NB Bovenstaande regel moet op 1 regel staan
Klik op **Save** (*Zorg ervoor dat Notepad geen extensie toevoegt!*)

3 Geef in het command-window de opdracht: gpg --edit-key KEYID waarbij KEYID je huidige GPG key id is. Je key id zijn de laatste acht karakters van je PGP key fingerprint. Bij mij is dat 38C66170.

4 Geef vervolgens de opdracht (dus binnen het gpg-programma):
setpref SHA512 SHA384 SHA256 SHA224 AES256 AES192 AES CAST5 ZLIB BZIP2 ZIP Uncompressed
Merk op: opnieuw geldt dat bovenstaande opdracht als één onafgebroken regel moet worden gegeven.

5. Klik op **Save**

6 Terug in het command window, geef de opdracht: gpg --send-keys KEYID
(met wederom KEYID vervangen door de key id van je eigen PGP public key)

Zoals bekend, heeft ook de RUG een eigen PGP key, die wordt gebruikt om de public keys van haar medewerkers als zijnde authentiek te signeren. Deze RUG-CA-master-pgp key is inmiddels ook aangepast. Met de opdracht gpg --keyserver pgp.surfnet.nl --recv-keys 3FA21196 kan de RUG-CA-master-pgp key aan je public keyring worden toegevoegd. Als dat al niet is gebeurd, signeer die key dan en geef hem trust-setting full.

Nieuwe PGP key

Op termijn dienen ook de PGP keys zelf te worden vervangen door sterkere keys. Dat is even vervelend, maar het is als bij de tandarts: beter een klein gaatje nu vullen dan wachten totdat de schade zo groot is dat de tand eruit moet. Op zich is het een eenvoudige operatie, maar er is wat nazorg nodig.

Om te beginnen krijgt ook de RUG een nieuwe RUG-CA-master-pgp key. Die is er al en kan nu al worden toegevoegd aan je public keyring: gpg --keyserver pgp.surfnet.nl --recv-keys 2909DB50

Deze key heeft als fingerprint 152D 4490 32DE CFDE AF01 B155 13C5 5004 2909 DB50. Controleer dat, signeer de key vervolgens en geef hem eveneens trust-setting full.

Vervolgens kan er (in Thunderbird) een nieuwe PGP key worden gemaakt:

1 Open het Key Management-menu
2 Selecteer **Generate** -> **New Key Pair**
3 Onder de Advanced Tab (ongeveer halverwege in het window) selecteer **Key type RSA** en **Key lengte 2048**.
4 Volg de standaardprocedure voor het genereren van een nieuwe key. Suggestie: deze key is van jezelf, je kunt dezelfde passphrase hanteren als die welke voor je huidige key wordt gebruikt.
5 Signeer je nieuwe GPG key met je oude key (niet omgekeerd!).
6 Signeer de nieuwe RUG-CA-master-pgp key met je nieuwe GPG key.
7 Stuur je nieuwe PGP public key naar de PGP keyservers en vraag Anke Breeuwsma, Hopko Meijering, Frans Velthuis of mij om je nieuwe PGP key namens de RUG te signeren. Als je oude key al door de RUG was gesigneerd en als je zelf je nieuwe key met je oude key hebt gesigneerd, dan kan dat zonder dat nadere authenticatie nodig is. Je hoeft dan dus niet meer je pas of rijbewijs te laten zien.

Een wat langer verhaal dan gebruikelijk, maar preventief onderhoud is belangrijk. Stel het niet uit. Een uitgebreidere toelichting volgt binnenkort op de website.

Vragen en opmerkingen kunnen natuurlijk altijd worden gesteld aan:

Frank B. Brokken
--altijd preventief onderhoudend bezig--

- Moore's Law over de trend in de toename van rekenkracht: **http://en.wikipedia.org/wiki/Moore's_law**
- Meer informatie over security: **www.rug.nl/cit/security**
- Meer informatie over PGP key: **www.debian-administration.org/users/dkg/weblog/48**