Annual Security Award 2006

Frank Brokken
f.b.brokken@rug.nl

ICT-security

Frank Brokken is security manager bij het RC. 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.

Begin januari werd voor de vierde keer de RUG Annual Security Award uitgreikt. Er staat expliciet 'RUG Annual Security Award' omdat het Security Award-initiatief inmiddels ook elders is overgenomen. SURFnet heeft dit jaar, in navolging van 'onze' Annual Security Award een 'Nationale SURFnet Security Award' in het leven geroepen. Het bestaan van een Nationale Security Award betekent niet het einde van onze eigen Security Award. Integendeel: lokale aandacht voor het positieve aspect van ICT Security blijft belangrijk en kan ook goed als springplank naar de Nationale Security Award worden gebruikt.

De inzendingen

Dit jaar werden via de website drie bijdragen ontvangen. Casper Bodewitz, werkzaam bij de unit Applicatieontwikkeling van het RC, stuurde een bijdrage die voortbouwt op de inzichten van de Medische Faculteit van vorig jaar om een veilige ontwikkelomgeving te realiseren waarin productiviteit en veiligheid beide kunnen worden gerealiseerd.
Ook de inzending van de Medische Faculteit borduurde voort op de benadering die al eerder tot het toekennen van de Annual Security Award heeft geleid (het isoleren van een werk/ontwikkelomgeving) met de introductie van een methode om toetsen en tentamens elektronisch veilig aan te bieden en af te nemen.
Adri Mathlener, werkzaam bij de unit Werkplekbeheer van het RC deed mee aan de competitie met een bijdrage die zich richtte op een groeiend probleem: het onthouden en bedenken van wachtwoorden.

Sterke passwords

De Annual Security Award der Rijksuniversiteit Groningen werd op 8 januari j.l. door prof. dr. C.G.M. Sterks, directeur van het RC, toegekend aan Adri Mathlener vanwege de zeer brede toepasbaarheid van de password-beheersapplicatie waarop door zijn bijdrage is gewezen. Bij de uitreiking werd door professor Sterks opgemerkt:
"Het beheer van een veelheid van passwords is voor veel gebruikers een groeiend probleem, en een standaard beschikbare beheersapplicatie maakt het dan mogelijk om te allen tijde, sterke passwords te gebruiken voor elk systeem waarop de gebruiker een account heeft, ook wanneer een password bij herhaling moet worden veranderd. De door Adri voorgestelde aanpak kan door vrijwel elk lid van onze universitaire gemeenschap worden overgenomen en overwogen kan worden zijn beheersapplicatie op te nemen in de Universitaire werkplek."

De prijsuitreiking

Tot zover professor Sterks. Adri Mathlener is vervolgens uitgenodigd om zijn bijdrage in deze column inhoudelijk toe te lichten.

Frank B. Brokken
(maakt gebruik van prima passwords)

KeePass

Adri Mathlener a.l.mathlener@rug.nl

Met de opkomst van bedrijfsnetwerken en internet is het gebruik van wachtwoorden gemeengoed geworden. Het is niet verstandig om hiervoor gebruik te maken van slechts 1 wachtwoord. Als dit wachtwoord op straat komt te liggen is de schade en bijkomende ellende meestal niet te overzien. Dit nemen vele gebruikers toch voor lief en men gaat er van uit dat het hun niet zal overkomen.

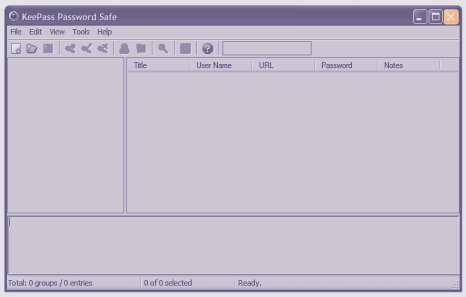
Sterk wachtwoord

Nu is het voor velen een probleem om een groot aantal verschillende wachtwoorden te onthouden. En met verschillende bedoel ik dus niet wachtwoorden in de trend van 'geheim01', 'geheim02' enzovoort. Een andere voorwaarde die aan een wachtwoord moet worden gesteld, is dat het moeilijk te raden is. Hoe sterker het wachtwoord des te moeilijker het is te raden.
De sterkte wordt bepaald door de lengte, gebruik van kleine letters, hoofdletters en andere tekens. Door nu van een bepaalde zin de eerste letters te nemen, kom je al een heel eind. Een voorbeeld van een sterk wachtwoord is de zin: 'Altijd Is Kortjakje Ziek Maar Eenmaal Per Week Niet #'. Hiermee kan het volgende wachtwoord gevormd worden: 'a1kzm1Xpwn#'.

De 'I' is vervangen door een '1' en daarnaast is 'eenmaal' vervangen door '1X'. De sterkte wordt ook nog bepaald door de spreiding van de afzonderlijke letters en tekens over het toetsenbord.

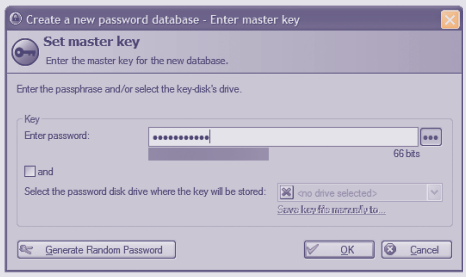
Open Source

Blijft echter over het onthouden van al dit soort zinnen; dat is en blijft een lastig punt. Hier komt nu het programma KeePass[1] van pas. Het is uitgebracht als Open Source en kan zonder kosten worden gebruikt onder Windows, Linux, Mac OS-X en draait eveneens op PocketPC, Palm en Smart Devices. Tevens is er een versie beschikbaar voor U3 USB-Sticks[2].
De installatie van KeePass is zeer eenvoudig: er hoeft slechts één *executable* te worden opgestart.



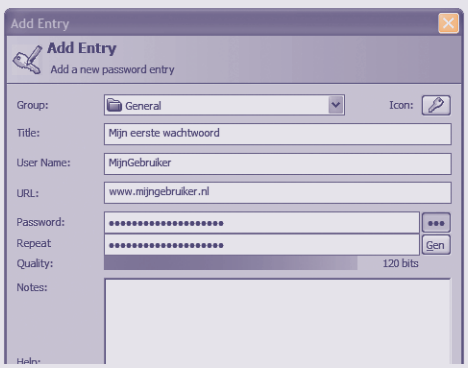
Figuur 1. Openingsvenster

Als eerste stap dient de database te worden aangemaakt waarin alle wachtwoorden worden opgeslagen. De database wordt met de master key versleuteld. We gebruiken hier het eerder bedacht wachtwoord: 'a1kzm1Xpwn#'. Om fouten uit te sluiten, wordt nogmaals om de master key gevraagd. Wanneer u deze vergeet, is er echt geen enkele mogelijkheid om de database weer te openen! De database wordt via AES[3] versleuteld.



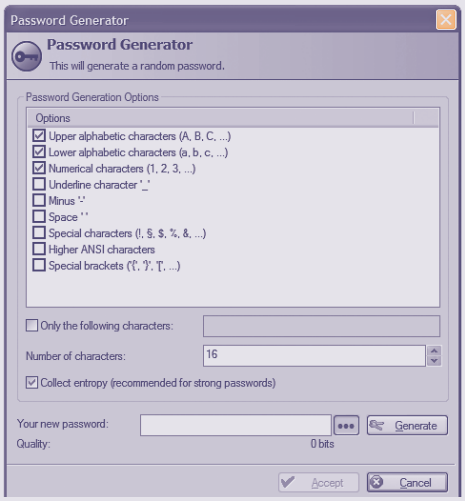
Figuur 2. Invoeren van de master key

U kunt nu de passwords die u in gebruik heeft onderbrengen in verschillende groepen.



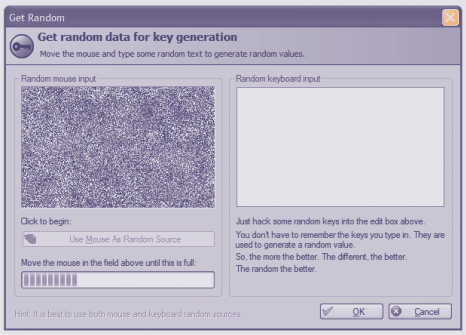
Figuur 3. Toevoegen van een wachtwoord

KeePass is u van dienst bij het bedenken van een wachtwoord . U kunt aangeven aan welke voorwaarden het wachtwoord moet voldoen.



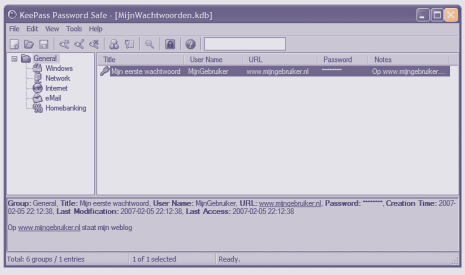
Figuur 4. Wachtwoord generator

De randomgenerator zorgt er nu voor dat er een willekeurig wachtwoord wordt gegenereerd dat aan uw voorwaarden voldoet.



Figuur 5. Randomgenerator

Het wachtwoord is nu beschikbaar voor gebruik. Door gebruik te maken van keyboard shortcuts is het mogelijk de usernaam, de url en het wachtwoord in het clipboard te plaatsen en kan het in het door u gewenste programma worden gebruikt. KeePass draagt er zorg voor dat de benodigde data slechts kort beschikbaar is in het clipboard. Standaard staat deze tijd op tien seconden, maar is naar believen aan te passen.



/Figuur 6. Overzicht

De database waar alle wachtwoorden in worden opgeslagen, staat op uw harddisk, maar deze kunt u natuurlijk ook als backup op een usb-stick zetten. Daarnaast biedt KeePass de mogelijkheid om de database naar verschillende formaten te exporteren. De exportfiles zijn gewoon leesbaar, dus let goed op waar u deze exportfiles opslaat.

Links

- Informatie en deelname RUG Annual Security Award: **www.rug.nl/rc/security/award/competitie**
- Meer over de nationale security award, de SURFnet-CERT Security Award: **http://cert-nl.surfnet.nl/award**

noot

1 www.keepass.info
2 www.u3.com
3 http://en.wikipedia.org/wiki/Advanced_Encryption_Standard