KeePass Password Safe 2.18

A light-weight easy-to-use password manager

Systeemvereisten:
Windows 98 / 98SE / ME / 2000 / XP / 2003 / Vista / 7 / 8, 32-bit / 64-bit, Mono (Linux, Mac OS X, BSD, ...). Microsoft .NET Framework ≥ 2.0 (reeds opgenomen in Windows Vista en hoger) of Mono ≥ 2.6.

Freeware, Open source (GPL v.2)	**Ontwikkeld door:**	Dominik Reichl http://keepass.info
	Contactpersoon:	Dirk.Deridder@smals.be

Functionaliteiten

Er gaat geen dag voorbij of je krijgt tips over het gebruik wachtwoorden. Ze moeten langer zijn, niet gemakkelijk te raden, best een aantal speciale karakters bevatten, ... Bovendien zijn ze best verschillend voor elke website of toepassing die je gebruikt. Dit maakt het in de praktijk niet gemakkelijk om ze te onthouden, zelfs wanneer je een of ander mnemonisch systeem gebruikt (bijv. een zinsnede waar je de letters van de toepassing aan toevoegt op bepaalde plekken). Ook het groot aantal websites en toepassingen, elk met hun eigen gebruikersgegevens (accounts, email adressen, privé/werk, ...) zijn door de vaak erg uiteenlopende systemen van gebruikersidentificatie moeilijk te beheren.

KeePass Password Safe is een excellent hulpmiddel om je te helpen om al deze gegevens te beheren. Hiervoor gebruikt het een geëncrypteerde databank (mbv. AES en het Twofish algoritme) waarin alle gegevens veilig opgeborgen worden. De toepassing kan je ook helpen om nieuwe wachtwoorden te genereren waardoor je niet hoeft te twijfelen bij de eerstvolgende “create new account” missie op het web.
Aan de hand van een “master” wachtwoord kan je toegang krijgen tot je KeePass databank. Vervolgens kan je bijv. een gebruikersaccount selecteren en het wachtwoord zal naar je clipboard verhuizen. Op die manier hoef je het wachtwoord niet over te tikken, een simpele plak-operatie volstaat. Na een zelf in te stellen tijd zal KeePass er ook voor zorgen dat het wachtwoord niet meer in de plak-buffer staat en dat de toegang tot KeePass zelf opnieuw het “master” wachtwoord vereist. Op die manier blijft alles veilig opgeborgen.

KeePass Password Safe kan op twee manieren gebruikt worden: via een lokale installatie of via een installatie op een USB stick. Dit laatste laat toe om je wachtwoordenkluis mee te nemen en te gebruiken op eender welk systeem. Let hierbij wel op dat een zogenaamde “keylogger” je “master” wachtwoord kan registreren en zo (indien men ook je KeePass databank kan copieren) toch nog toegang kan krijgen tot je gegevens. Om dit te vermijden voorziet KeePass in een manier om verschillende “master” wachtwoord systemen te combineren alsook het gebruik van een Secure Desktop. Deze laatste optie gaf wel problemen in de test op Windows 7. Dit is een gekend probleem en mogelijk komt er in de nabije toekomst een update.

Conclusies en Aanbevelingen

Vermijd het noteren van wachtwoorden in schriftjes of post-it’s. Wil je een gemakkelijke manier om een groot aantal van deze gegevens te beheren, kies dan resoluut voor een tool zoals KeePass. In het verleden verscheen ook een review van een vergelijkbaar hulpmiddel LastPass 1.73. Ook dit programma blinkt uit in haar eenvoud.

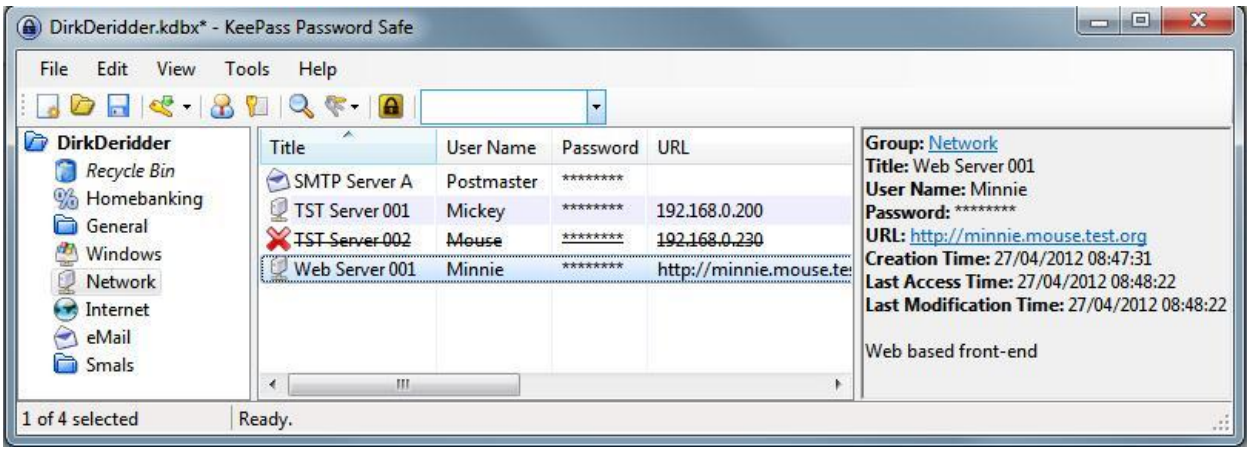
Het feit dat dit een open source initiatief (OSI Certified) is kunnen we alleen maar toejuichen. Je kan er immers op rekenen dat tools zoals deze serieus onder de loep genomen zijn door tal van beveiligingsexperts.

Testen en Resultaten

KeePass 2.18 werd geïnstalleerd op Microsoft Windows 7 volgens de instructies op de website. Merk op dat er twee versies bestaan van dit product: een klassieke editie met een beperkt aantal functies, en een uitgebreidere professionele editie. Ook deze laatste blijft overigens erg spartaans in de aangeboden functionaliteit, maar dat is een goede zaak. In deze test gebruikten we de professionele editie en hebben we er voor gekozen om deze lokaal te installeren ipv op een USB stick (gebruik hiervoor de Portable KeePass versie). Tijdens de test zijn er geen problemen genoteerd qua stabiliteit behalve dan het probleem met de Secure Desktop optie.

De eerste stap na de installatie is de creatie van een databank. Hiervoor vraagt KeePass een "master" wachtwoord waarbij je best kiest voor een erg sterk wachtwoord (tips). Verder kan je dit aanvullen met een key-file (bijv. een zelfgekozen bestand op een USB stick waarvan KeePass de inhoud gebruikt voor de authentificatie) en je normale windows account. Door deze drie methodes te combineren kan je de beveiliging van je gegevens erg hoog instellen. De gebruikte encryptietechnieken voor de databank zijn standaard (AES en Twofish) en zeker afdoende. Hou er wel rekening mee dat je bij verlies van het "master" wachtwoord (of bijv. je key-file) geen toegang meer kan krijgen tot al je gegevens.

De tweede stap is het opvullen van de databank met al je gegevens. Het is mogelijk deze te organiseren in een handige folderstructuur. Je kan ook icoontjes toekennen aan de verschillende entries. Verder is er een handige zoekfunctie die toelaat om snel de juiste gegevens terug te vinden. Er zijn diverse keyboard shortcuts om bijv. een entry aan te maken, het paswoord te copiëren, de bijbehorende url te openen in een browser, ... Het is ook mogelijk om bij de wachtwoorden een vervaldatum op te geven. Wanneer een wachtwoord vervalt dan zal KeePass dit duidelijk aangeven zoals in de screenshot onderaan voor "TST Server 002".



Gebruiksvoorwaarden

KeePass Password Safe 2.18 is volledig vrij te gebruiken en valt onder een GPL v.2 licentie.