Passwortsicherheit

Sicherer Freund und Helfer

Die Juli-Ausgabe von Datenschutz PRAXIS hat gezeigt, wie man Passwörter in der Kombination Windows Desktop/PocketPC sicher speichern kann. Diesmal stellen wir Ihnen eine vergleichbare Kombination für Palm OS vor, Keyring for Palm OS.

Keyring ist eine kostenlose und ausgesprochen kompakte Anwendung, die auf einem Gerät mit Palm OS (ab Version 3.0) läuft. Hauptzweck der Software ist, Passwörter, PINs und andere wichtige Codes an einem geschützten, digitalen Ort sicher aufzubewahren. Damit gehören das Vergessen der vielen verschiedenen PINs und das Notieren von Passwörtern an vermeintlich unauffälligen Plätzen der Vergangenheit an.

So installieren Sie Keyring

Synchronisieren Sie die Dateien keyring-1.2.3-de.prc, MDLib.prc und DESLib.prc aus der heruntergeladenen ZIP-Datei auf den Palm. Beim ersten Start legt das Programm automatisch eine leere Datenbank mit dem Namen Keys-Gtkr.pdb an. Dabei fragt es Sie nach dem gewünschten Master-Passwort für die Datenbank. Zur Sicherheit müssen Sie es zweimal eingeben.

Mit der Qualität dieses Master-Passworts steht und fällt die Sicherheit der Datenbank!

So arbeitet Keyring

Namensfelder wie z.B. „Deutsche Bank“ oder „GMX“ werden in der Datenbank ebenso wie die Kategorien – z.B. „Firma“ – unverschlüsselt gespeichert. Achten Sie also darauf, dass die Informationen dort unverfänglich sind.

Die Konto-, Passwort- und Kommentarfelder sind dagegen voll verschlüsselt. Keyring nutzt dazu das Triple-DES-Verfahren. Es gilt mit einer Schlüssellänge von 112 Bit als sicher.

Der 128-Bit-MD5-Hash des Master-Passworts wird in zwei 64-Bit-Schlüssel K1 and K2 aufgespaltet.

Keyring-Download

Unter www.datenschuetzer.de können Sie Software und Editor bequem herunterladen. Klicken Sie auf der Startseite auf den Punkt „Downloads“ und dann auf „Goodies“.

Links ist eine Übersicht der Namensinträge zu sehen. Diese Übersicht ist auch ohne Passworteingabe sichtbar. Das geschlossene Schloss oben rechts zeigt, dass kein Passwort eingegeben wurde. Nach Eingabe des Master-Passworts können Sie den kompletten Eintrag lesen (rechts).

Da der DES-Algorithmus jeweils ein Bit eines jeden Bytes ignoriert, ergibt dies zwei 56-Bit-Schlüssel, zusammen also 112 Bit. Diese werden in der Triple-DES-Variante Encrypt(K1, Decrypt(K2, Encrypt(K1, Daten))) verwendet. Jeder 8-Byte- Input-Block wird dabei mit dem gleichen Schlüssel verschlüsselt (ECB-Modus).

So bedienen Sie Keyring

Rufen Sie das Programm auf, erhalten Sie eine Liste mit den unverschlüsselten Namenseinträgen. Möchten Sie die Details zu einem Eintrag lesen, müssen Sie das Master-Passwort eingeben. Es lässt sich für eine einstellbare Zeit speichern. Während dieser Zeit müssen Sie es dann nicht neu eingeben. Ein Schloss in der rechten oberen Ecke der Anwendung zeigt an, ob Sie eingeloggt sind oder nicht.

So generieren Sie neue Passwörter

Über die Taste „Generieren“ können Sie ein neues Passwort für den jeweiligen Eintrag erzeugen. Die Länge des Passworts und die Komplexität lassen sich einfach konfigurieren.

Ein sicherer Allrounder!

Keyring gibt Ihnen die Möglichkeit, Passwörter, PINs und dergleichen auf einem Palm-OS-Gerät sicher zu speichern. Es bietet Versionen in mehr als zehn Sprachen und einen plattformunabhängigen Editor für den Desktop-Rechner oder das Notebook.

Eine neue Version mit verbesserter Verschlüsselung (AES256) ist in Vorbereitung. Sie können eine Vorabversion testen; der Autor rät derzeit allerdings noch vom Einsatz ab.

Prof. Dr. Rainer W. Gerling

Weiterführende Infos unter:

http://gnukeyring.sourceforge.net

http://www.ict.tuwien.ac.at/keyring