



Presseinformation

Darmstadt,
den 26. Februar 2007

Passwörter, PINs, TANs & Co. to-go – Handy hütet Geheimnisse

CeBIT: Fraunhofer-Institut zeigt Software für sicheres und bequemes Geheimnis-Management. MobileSitter schützt Passwörter und Zahlencodes auf Mobiltelefon und PDA

Am Geldautomat, im Büro, im Online-Shop oder bei der Internet-Auktion, überall sichern Passwörter und PINs den Zugang und ständig werden es mehr. Nach einer aktuellen Bitkom-Umfrage müssen die meisten Menschen sich heute rund 20 Zahlen- oder Zeichenkombinationen merken, manche Menschen sogar bis zu 60. Damit nicht genug, müssen viele dieser geheimen Codes regelmäßig geändert werden. Um Nutzer vor dem Vergessen von Geheimnissen zu bewahren und Zugangsdaten zu schützen, haben Entwickler am Fraunhofer-Institut SIT eine Software für das Handy entwickelt, die Geheimnisse angriffssicher verschlüsselt und die Zugangsinformationen jederzeit zur Verfügung stellt. Mit dem MobileSitter muss der Nutzer sich nur noch ein Master-Passwort merken, um alle seine PINs und Passwörter, ja sogar TANs und i-TANs sowie Log-In-Informationen, sicher zu verwalten. „Im Gegensatz zu anderen Produkten bietet der MobileSitter hohe Sicherheit und Benutzerfreundlichkeit“, sagt Projektleiter Ruben Wolf, „die Software wird einen Angreifer, der an die abgespeicherten Geheimnisse gelangen möchte, zur Verzweiflung treiben. Der rechtmäßige Nutzer wird hingegen bei der Eingabe des richtigen Master-Passworts durch eine Bildanzeige, einen so genannten optischen Rückkanal, unterstützt.“ Die Fraunhofer-Forscher zeigen die Software erstmals vom 15. bis zum 21. März auf der Computermesse CeBIT in Hannover (Halle 7, Stand D22/10).

Oliver Küch
Fraunhofer-Institut für
Sichere Informationstechnologie
Presse und Öffentlichkeitsarbeit

Rheinstraße 75
64295 Darmstadt
Telefon +49 (0) 6151/8 69-2 13
Telefax +49 (0) 6151/8 69-2 24
email: presse@sit.fraunhofer.de
www.sit.fraunhofer.de

Um die wichtigen Informationen auch bei Verlust des Handys zu schützen, haben die Forscher ein neues Verfahren entwickelt, das auf dem weltweit

anerkannten Verschlüsselungsverfahren AES 128 basiert und bereits zum Patent angemeldet wurde. „Als Angreifer kann man die verschlüsselten Daten eines Handys leicht von einem Mobiltelefon auf einen Rechner übertragen und dort mit speziellen Hackertools Hunderttausende Master-Passwörter innerhalb einer Sekunde ausprobieren“, so Wolf. „Wenn der Angreifer feststellen kann, ob ein getestetes Master-Passwort falsch oder richtig war, wie dies bei anderen Produkten oftmals der Fall ist, kann er unter Umständen das korrekte Master-Passwort ermitteln und somit an alle Geheimkombinationen gelangen.“ Manche Lösungen zeigen zwar keine Fehlermeldungen, schränken die Menge der Möglichkeiten für das Master-Passwort jedoch stark ein oder bestätigen die richtige Eingabe des Master-Passworts durch Anzeige einer weiteren Zeichenfolge. „Das alles liefert einem Angreifer unter Umständen wichtige Informationen und erleichtert ihm die Arbeit“, sagt Wolf. Beim MobileSitter hingegen ist die Anzahl möglicher Master-Passwörter praktisch unbegrenzt. Bei Eingabe des richtigen Geheimnisses zeigt die Software eine Grafik, die der Benutzer problemlos wiedererkennt, aber dem Angreifer keinerlei Rückschlüsse auf das gewählte Master-Passwort erlaubt.

Bei Eingabe eines falschen Master-Passworts liefert der MobileSitter keine Fehlermeldungen, sondern generiert falsche Passwörter, die jedoch nicht als solche zu erkennen sind. „Ein Angreifer, der das richtige Geheimnis nicht kennt, kann also nicht erkennen, dass es falsche Codes sind,“ so Wolf, „ganz gleich, ob es sich um TANs, TAN-Listen, PINs oder Passwörter handelt.“ Mit den heutigen technischen Möglichkeiten haben Angreifer deshalb keine Chance, an die Geheimnisse des MobileSitters zu gelangen. Nutzern hingegen bieten einstellbare Password-Policies, die Unterstützung von Passwort-Änderungen und Im- und Exportfunktionen nicht nur mehr Sicherheit, sondern auch besseren Komfort.

Im Gegensatz zu existierenden Produkten lassen sich mit dem MobileSitter beliebig viele Geheimnisse verwalten und diese auch von einem Gerät auf ein anderes übertragen. Der Nutzer kann PINs und TANs zum Beispiel auf dem Handy und dem heimischen PC nutzen. Bei Neukauf oder Verlust eines Handys oder Rechners lassen sich Zugangscodes einfach importieren. Die Software wurde speziell für mobile Endgeräte entwickelt und funktioniert auf PCs, Handys und PDAs, die Java ME unterstützen und

mindestens eine Display-Breite von 160 Pixeln besitzen. Auf der CeBIT zeigt das Fraunhofer-Institut noch einen Prototyp. Schon bald wird die Software unter www.sit.fraunhofer.de oder www.mobilesitter.de für rund zehn Euro per Lizenz erhältlich sein.

4211 Zeichen, Abdruck frei, Beleg erbeten

Sollten Sie keine Pressemitteilungen vom SIT wünschen, senden Sie eine entsprechende E-Mail an presse@sit.fraunhofer.de