

Tricks und Tools mit hohem Risiko

Weil sich kaum jemand alle Zugangs-codes merken kann, versuchen viele mit Tricks oder technischen Hilfsmitteln, sich die Verwaltung der eigenen Geheimkombinationen zu erleichtern. Doch die herkömmlichen Hilfsmittel sind nicht für alle Situationen geeignet und bieten oft auch nicht genug Sicherheit. Braucht man seine PIN etwa am Geldautomaten, hilft ein Passwort-Tool auf dem Computer zuhause wenig. Und auch USB-Sticks und andere mobile Datenträger, auf denen sich Geheimkombinationen gesichert ablegen lassen, versagen an der Supermarktkasse, weil man sie ohne Zusatzgerät gar nicht benutzen kann.

So bleibt für viele nur der berühmte Zettel, auf dem man sich seine Geheimkombinationen notiert, oder die Speicherung auf dem eigenen Mobiltelefon. Beides ist jedoch äußerst riskant, denn genauso schnell wie ein Zettel mit Geheimkombinationen in die falschen Hände gelangen kann, kommen Datendiebe an Passwörter und PINs auf dem Handy, selbst wenn sie verschlüsselt wurden. Mit speziellen Computerprogrammen und leistungsfähigen Rechnern sind Hacker in der Lage, innerhalb von Sekunden Millionen von Master-Passwörtern bzw. Schlüsseln auszuprobieren und an alle hinterlegten Geheimnisse zu gelangen.

Hohe Angriffssicherheit

Herkömmliche Programme zur Geheimnisspeicherung helfen Angreifern oft, indem sie bei einem fehlgeschlagenen Entschlüsselungsversuch eine auch für Unberechtigte verständliche Fehlermeldung geben. Mit jeder solchen Meldung gelangt ein Hacker näher ans Ziel.

Der MobileSitter verhält sich ganz anders: Auch seine Nutzer müssen sich ein Master-Passwort merken, mit dem alle weiteren Geheimnisse verschlüsselt werden. Doch gerät das Mobiltelefon in die falschen Hände und ein Unberechtigter versucht, durch wiederholtes Austesten von Master-Passwörtern an die sicher hinterlegten Geheimkombinationen zu gelangen, dann verursacht dies keine Fehlermeldungen, die für Unberechtigte verwertbar sind.

Während andere Produkte das eingegebene Master-Passwort auf Korrektheit überprüfen und dem Anwender das Ergebnis dieser Überprüfung mitteilen (z.B. "Eingegebenes Master-Passwort nicht korrekt"), akzeptiert der MobileSitter jede denkbare Kombination eines Master-Passworts und berechnet auf Basis dieser eingegebenen Master-Passwörter entsprechende Geheimkombinationen, bei denen ein Unberechtigter zunächst nicht entscheiden kann, ob es sich um die korrekten Geheimkombinationen handelt oder nicht. Nach Eingabe eines Master-



Das Master-Passwort lässt sich bequem über die Bewegungstasten des Mobilfunkgeräts eingeben.

die tatsächlichen Geheimkombinationen handelt, bleibt dem Hacker nichts anderes übrig, als das Entschlüsselungsergebnis bei der jeweiligen Stelle einzugeben (z.B. Geldautomat, Bezahlung an der Kasse, Betriebssystemanmeldung), wo er bei falscher Geheimkombination abgewiesen wird.

Da die Anzahl der potenziell möglichen Master-Passwörter praktisch unbegrenzt ist, hat ein Hacker, der sich unberechtigt Zugriff zu einem Mobiltelefon mit MobileSitter verschaffen kann, nichts gewonnen. Selbst wenn das eigene Master-Passwort in den Listen der Hacker-Tools enthalten ist, kann ein Hacker nicht erkennen, dass der Benutzer ein solch schwaches Master-Passwort verwendet.

Passworts liefert der MobileSitter grundsätzlich solche Entschlüsselungsergebnisse, welche den Bildungsregeln der jeweiligen Geheimkombinationen genügen, z.B. durch ausschließliche Verwendung von Ziffern bei PINs oder durch Berücksichtigung von Passwortregeln.

Gibt also ein Hacker ein Master-Passwort ein, dann liefert der MobileSitter immer solche Entschlüsselungsergebnisse, welche für den Hacker so aussehen, als könnte es sich dabei um die sicher hinterlegten Geheimkombinationen handeln. Um wirklich entscheiden zu können, ob es sich bei einem Entschlüsselungsergebnis um

Der rechtmäßige Anwender erkennt hingegen sofort, ob er sein korrektes Master-Passwort eingegeben hat. Hierzu zeigt der MobileSitter dem Anwender ein vom Master-Passwort abhängiges Symbol an, das sich leicht wiedererkennen lässt. Einem Hacker hingegen hilft die durch das Bild übermittelte Rückmeldung nicht weiter.



MobileSitter

www.mobilesitter.de

Sicheres Geheimnis-Management für Handy und PDA

Ob am Computer, am Geldautomaten oder an der Supermarktkasse – ohne Passwörter, PINs oder TANs geht meist gar nichts mehr. Je mehr Geheimnisse man sich merken muss, desto schwieriger wird es, sich an diese eigentlich bedeutungslosen Zeichenketten zu erinnern. Manche versuchen, den Fluch des digitalen Zeitalters los zu werden, indem sie für verschiedene Zwecke stets das gleiche Passwort verwenden, andere notieren die Geheimnisse auf Papierzettel. Wer das tut, hat seine Zugangscodes eher parat, geht damit jedoch auch Risiken ein.

Technische Hilfsmittel wie Passwort-Programme für den PC können das Risiko zwar verringern, lassen sich aber nicht unterwegs nutzen – der Fraunhofer-MobileSitter schon. Mit ihm muss sich der Nutzer nur noch sein Master-Passwort merken, der Rest seiner Geheimnisse wird auf dem Handy gespeichert und durch Verschlüsselungsverfahren und besondere Softwaregestaltung geschützt. Im Gegensatz zu bekannter Software lassen sich mit dem MobileSitter alle Arten von Geheimnissen speichern, Passwörter und PINs ebenso wie ganze TAN-Listen.

Flexible Technologie

Der MobileSitter wurde auf Basis von Java ME entwickelt. Dadurch kann er betriebssystemunabhängig auf verschiedenen Endgeräten installiert und benutzt werden. Zur Verwendung auf Mobiltelefonen wurden die Standards CDLC 1.1 und MIDP 2.0 eingesetzt. Der Dateizugriff basiert auf dem Standard JSR 75. Darüber hinaus sollte das Display eine Mindestbreite von 160 Pixeln haben.

Zur Verschlüsselung der Geheimkombinationen (Passwörter, PINs und TANs) wird ein spezielles für den MobileSitter entwickeltes Verfahren angewendet. Dieses Verfahren basiert auf weltweit anerkannten Standards wie AES 128, PKCS#5 und ISO/IEC 9797-1.

Viele Anwendungsmöglichkeiten

Mit dem MobileSitter lassen sich beliebige Geheimkombinationen auf mobilen Endgeräten verwalten – seien es Passwörter, PINs oder ganze TAN-Listen. So kann man seine Geheimkombinationen immer und überall nutzen – an Computer oder Telefon, zuhause oder im Büro, beim Bezahlen im Restaurant ebenso wie beim Einkauf im Supermarkt oder Internet. Nutzer des MobileSitters müssen sich nur noch ein einziges Passwort merken, das Master-Passwort. Alle anderen Geheimkombinationen sind sicher abgespeichert.

Der MobileSitter entstand im Rahmen eines Forschungsprojekts am Fraunhofer-Institut für Sichere Informationstechnologie (SIT) und wird als Produkt vertrieben. Der MobileSitter lässt sich sowohl in Unternehmen als auch privat einsetzen. Folgende Akteure können im professionellen Kontext von MobileSitter profitieren:

- ++ Unternehmen, die ihren Angestellten eine Lösung zum sicheren Management von Geheimkombinationen zur Verfügung stellen möchten. Dadurch lässt sich die Unternehmenssicherheit an einer kritischen Schwachstelle deutlich verbessern.
- ++ Hersteller von mobilen Endgeräten, welche den MobileSitter in ihre Produkte integrieren möchten.
- ++ Anbieter von Mobilkommunikationsdiensten, welche den MobileSitter in ihre Produkte integrieren möchten.
- ++ IT-Dienstleister, die den MobileSitter als Vertriebspartner für das Fraunhofer-Institut SIT bei ihren Kunden vertreiben möchten.

Personen, die den MobileSitter gerne privat einsetzen möchten, können diesen im Online-Shop des Fraunhofer-Instituts SIT käuflich erwerben.