

MOBILESITTER
SICHERE PASSWORT-VERWALTUNG
FÜR SMARTPHONES



MobileSit⁺ter

MOBILESITTER



Ob für E-Mail, E-Commerce, Web 2.0 oder Bankgeschäfte – ohne Passwörter, PINs oder TANs geht heute meist gar nichts. Doch je mehr Zugangscodes wir uns merken müssen, desto schwieriger wird es. Passwort-Manager erleichtern Nutzern den Alltag, aber viele der vermeintlich sicheren Programme sind für Angreifer leichte Beute – selbst wenn sie anerkannte Verschlüsselungsverfahren einsetzen. Anders der Fraunhofer-MobileSitter: Er schützt Passwörter, PINs und TAN-Listen durch ein innovatives Verfahren, das wesentlich mehr Sicherheit bietet als herkömmliche Software. Nutzer freuen sich über kinderleichte Bedienung der Handy-Software, Angreifer verzweifeln, weil der MobileSitter typische Passwort-Attacken wirksam vereitelt.

Mit dem MobileSitter muss man sich nur noch ein Master-Passwort merken, den Rest erledigt die Software. Gibt man das eigene Master-Passwort korrekt ein, werden alle gespeicherten Passwörter, PINs und TANs entschlüsselt und dem Benutzer angezeigt. Die Software lässt sich auf den meisten Smartphones installieren, so dass man seine Passwörter immer dabei hat. Der MobileSitter eignet sich für Privatanwender ebenso wie für den Unternehmenseinsatz – selbst als Werbemittel.

Schwächen konventioneller Produkte

Trotz Verwendung anerkannter Verschlüsselungsalgorithmen weisen viele Passwort-Manager erhebliche Sicherheitslücken auf. Denn die Entwickler übersehen häufig eine wichtige Tatsache: Als sicher betrachtete Verschlüsselungsalgorithmen wie etwa AES (Advanced Encryption Standard) sind nämlich nur dann sicher, wenn jede mögliche Schlüsselkombination gleich wahrscheinlich ist. So umfasst der Schlüsselraum, also die Menge aller möglichen kryptographischen Schlüssel, bei AES insgesamt 2^{128} ($\approx 3,4 \cdot 10^{38}$) Elemente. Nimmt man an, dass ein Master-Passwort nicht mehr als 12 Stellen hat, dann beträgt die Anzahl der Möglichkeiten, die sich über die Tastatur eingeben lassen, jedoch lediglich $4,8 \cdot 10^{23}$ – das entspricht gerade mal $1,4 \cdot 10^{-13}$ Prozent ($\approx 0,00000000000014$ %) des AES-Schlüsselraums. Möchte ein Angreifer an verschlüsselte Geheimnisse herankommen, dann muss er also nur eine vergleichsweise kleine Menge von kryptographischen Schlüsseln ausprobieren. Mit den heute zur Verfügung stehenden Rechenkapazitäten kann diese Aufgabe unter bestimmten Bedingungen in sehr kurzer Zeit bewältigt werden. In der Praxis stellt sich die Ausgangssituation für Hacker sogar noch sehr viel günstiger dar, da unter den denkbar möglichen Kombinationen von Master-Passwörtern bestimmte mit höherer Wahrscheinlichkeit verwendet werden als andere. Nach einer Untersuchung von ElcomSoft sind ca. 40% aller geschäftlich genutzten Passwörter in einem Wörterbuch zu finden.^I Dementsprechend programmieren Angreifer ihre Hacker-Software so, dass sie zunächst alle Wörter eines Wörterbuchs ausprobieren (Wörterbuchangriffe).

Angriffsmethoden

Zur Durchführung solcher Wörterbuch- oder Brute-Force-Angriffe (dem Ausprobieren aller relevanten Möglichkeiten) nutzen Angreifer heute Hackersoftware, die praktisch jeder erwerben kann und die einfach zu bedienen ist.^{II} Wer sich nicht selbst die Hände schmutzig machen möchte, für den gibt es im Internet digitale Schlüsseldienste, die das Knacken von Passwörtern als Dienstleistung anbieten.^{III} Durch neue Technologien wie Cloud-Computing lässt sich zudem enorme Rechenleistung einkaufen, wodurch das Knacken von Passwörtern zukünftig noch einfacher, schneller und günstiger werden wird.^{IV} Bereits



heute können Angreifer in kürzester Zeit Milliarden von Kombinationen austesten. Dies geschieht oft, ohne dass der eigentliche Besitzer dieser Daten etwas davon mitbekommt und ohne dass weitere Sicherungsmechanismen greifen können. Einige Hersteller versuchen zwar, den Rechenaufwand für Ver-/Entschlüsselung künstlich zu erhöhen, um die Zahl der Versuche pro Minute bei Wörterbuch-/Brute-Force-Angriffen zu limitieren. Bei herkömmlichen Endgeräten mit begrenzter Rechenleistung – etwa Smartphones – sind diese Gegenmaßnahmen jedoch unbrauchbar, weil sie die Gebrauchstauglichkeit erheblich einschränken.

Der Clou

Wenn die Daten mit konventionellen Passwort-Managern verschlüsselt wurden, können Angreifer erkennen, ob ein Entschlüsselungsversuch erfolgreich ist oder nicht. Anders wenn die Daten mit dem Fraunhofer-MobileSitter verschlüsselt wurden; hier kann ein Angreifer am Entschlüsselungsergebnis nicht erkennen, ob der Versuch erfolgreich war oder nicht. Gleich welches Master-Passwort eingegeben wird, der MobileSitter akzeptiert jede Eingabe und entschlüsselt die gespeicherten Daten immer in Abhängigkeit vom eingegebenen Master-Passwort, ganz egal, ob das Master-Passwort korrekt ist oder nicht. Je nach eingegebenem Master-Passwort werden dann entsprechende Entschlüsselungsergebnisse angezeigt. Jedes entschlüsselte und ausgegebene Passwort sieht so aus, als ob es richtig sein könnte. Wird also beispielsweise eine hinterlegte PIN für eine EC-Karte entschlüsselt, dann wird es sich bei dem Entschlüsselungsergebnis immer um eine vierstellige Ziffernkombination handeln. Somit ist aus Sicht eines Angreifers – egal ob Hacker oder Hackersoftware – nicht zu unterscheiden, ob das eingegebene Master-Passwort gefunden wurde oder nicht. Für Hacker oder Hackersoftware scheint jeder Entschlüsselungsversuch erfolgreich zu sein. Dadurch werden Wörterbuch- oder Brute-Force-Angriffe wirksam vereitelt. Dem Angreifer bleibt somit nichts Anderes übrig, als die Korrektheit der Entschlüsselungsergebnisse dadurch zu überprüfen, dass er versucht, sich damit bei den jeweiligen Zugängen und Konten anzumelden bzw. PINs und TANs auszuprobieren. Dort greifen dann jedoch die üblichen Sicherheitsmechanismen nach

einer bestimmten Anzahl von Fehlversuchen, z. B. bei der EC-Karte nach drei Fehlversuchen. Der rechtmäßige Benutzer hingegen kann sofort erkennen, ob er sein Master-Passwort korrekt eingegeben hat oder ob er sich vertippt hat. Hierbei hilft ihm eine vom Master-Passwort abhängige Grafik. Diese dient dem Benutzer zur Rückversicherung, dass das eingegebene Master-Passwort korrekt ist. Der Angreifer kann die Grafik jedoch nicht interpretieren, da er das Symbol für die korrekte Eingabe weder kennt noch ermitteln kann.

Technik/Systemvoraussetzungen

Der MobileSitter wurde auf Basis von Java ME entwickelt. Dadurch kann er betriebssystemunabhängig auf verschiedenen mobilen Endgeräten installiert und benutzt werden. Zur Verwendung auf Mobiltelefonen wurden die Standards MIDP 2.0 / CLDC 1.1 eingesetzt, welche von den meisten Mobilgeräten unterstützt werden. Der Dateizugriff basiert auf dem Standard JSR 75. Darüber hinaus muss das Display eine Mindestbreite von 160 Pixeln haben. Zur Verschlüsselung der Geheimkombinationen (Passwörter, PINs und TANs) wird ein speziell für den MobileSitter entwickeltes und patentiertes Verfahren angewendet. Dieses Verfahren basiert auf weltweit anerkannten Standards wie AES-128, PKCS#5 und ISO/IEC 9797-1.

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 – am Computer, zuhause oder im Büro, beim Bezahlen im Restaurant ebenso wie beim Einkauf im



Eingabe des Master-Passworts im MobileSitter.

- I. ElcomSoft: Password Security Survey 2009. www.elcomsoft.com/surveys.html
- II. Heise Online: ElcomSoft knackt Passwörter nun auch mit Wortlisten.
www.heise.de/newsticker/meldung/ElcomSoft-knackt-Passwoerter-nun-auch-mit-Wortlisten-832342.html;
Heise online. Passwortknacker für iPhone-Backups. www.heise.de/security/meldung/Passwortknacker-fuer-iPhone-Backups-922983.html;
- III. Heise online. Passwort-Cracker als Bezahltdienst. www.heise.de/newsticker/meldung/Passwort-Cracker-als-Bezahltdienst-147107.html;
- IV. Heise online. Preiswert Schlüssel knacken in der Cloud.
www.heise.de/newsticker/meldung/Preiswert-Schlüssel-knacken-in-der-Cloud-848574.html;
- IX. Cloud-Dienst knackt WLAN-Passwörter. www.heise.de/lx/meldung/Cloud-Dienst-knackt-WLAN-Passwoerter-879888.html

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 lässt sich sowohl in Unternehmen als auch privat einsetzen. Im professionellen Kontext kann der MobileSitter interessant sein für:

- ++ 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, die den MobileSitter in ihre Produkte integrieren möchten. (Produktveredelung/-ergänzung)
- ++ Anbieter von Mobilkommunikationsdiensten, die den MobileSitter in ihre Produkte integrieren möchten (Erweiterung von Diensten).

++ IT-Dienstleister, die den MobileSitter als Vertriebspartner für das Fraunhofer-Institut SIT bei ihren Kunden vertreiben möchten.

++ Unternehmen, die ihren Kunden oder Geschäftspartnern die MobileSitter-Software als Präsent oder Werbegeschenk mit eigenem Branding zukommen lassen möchten. Diese Kunden werden das sehr nützliche und sichere Werkzeug täglich einsetzen und somit jeden Tag an den Spender erinnert. Dabei ist die Logistik zur Verteilung des MobileSitters sehr einfach (kostenfreier Download mit Gutschein-Code).

Weiterentwicklung

Der MobileSitter entstand im Rahmen eines Forschungsprojekts am Fraunhofer-Institut SIT. Die Software wird ständig weiterentwickelt. Derzeit wird an einer PC-Variante gearbeitet, mit der Nutzer die eigenen Daten bequem über die PC-Tastatur eingeben können. Auch eine Synchronisierung der Daten zwischen PC und Mobilgerät wird möglich sein. Darüber hinaus wird eine Version der Software für das iPhone und für das Betriebssystem Android entwickelt.

*Fraunhofer-Institut für Sichere
Informationstechnologie SIT*

*Kontakt:
Dr. Markus Schneider, Ruben Wolf
Rheinstraße 75
64295 Darmstadt*

*Telefon 06151 869-3371-60177
Fax 06151 869-224
markus.schneider@sit.fraunhofer.de
ruben.wolf@sit.fraunhofer.de*

www.mobilesitter.de