

Der PasswordSitter

Fraunhofer Institut für sichere Informationstechnologie (SIT)

<http://www.sit.fraunhofer.de>

<http://www.password-sitter.de>

Passwörter im Alltag

Ob privat oder im Beruf, überall braucht man heutzutage Passwörter. Sie dienen zur Sicherung des Zugangs zur Mailbox, zum Steigern bei Online-Auktionen, zu Online-Foren, zu elektronischen Zeitungsarchiven, wie auch zur Zugangssicherung im Unternehmensintranet beispielsweise zu Dokumentenmanagementsystemen, Datenbanken und zu Workflowmanagementsystemen, um nur einige Anwendungen zu nennen. Auch wenn Passwörter grundsätzlich ein angemessen hohes Sicherheitsniveau bieten können, so tragen die heutigen Rahmenbedingungen dazu bei, dass beim Passwortschutz in der Praxis durch die Überforderung von Computernutzern gewisse Sicherheitsrisiken entstehen können.

Die Sicherheit vieler Anwendungen und Dienste, welche Passwortverfahren einsetzen, setzt voraus, dass diese Passwortverfahren sicher sind. Insbesondere erfordert dies, dass Computernutzer mit ihren Passwörtern in angemessener Weise umgehen. Dabei hilft ihnen der bei Fraunhofer SIT entwickelte PasswordSitter, durch welchen das Passwort-Management sicherer und benutzerfreundlicher zugleich wird und durch welchen aus Unternehmenssicht Kosten eingespart werden können. Verwendet ein Computernutzer den PasswordSitter, dann muss er sich nur noch ein einziges Passwort —hier als Master-Passwort bezeichnet— merken, um an jedem Ort, zu jeder Zeit und an jedem Computer alle seine Passwörter verfügbar zu haben. Da der PasswordSitter die Erzeugung der Passwörter für die jeweiligen Dienste und Anwendungen übernimmt, kann garantiert werden, dass diese Passwörter die allgemeinen Sicherheitsansprüche und auch die spezifischen Regeln des Dienstes bzw. der Anwendung erfüllen. Der PasswordSitter basiert auf einem neuen Verfahren, welches bei Fraunhofer SIT entwickelt wurde und dem Patentamt zur Patentierung vorliegt.

Probleme rund um Passwörter

Grundsätzlich sollten sich Benutzer stets geeignet starke Passwörter auswählen, die von anderen mit genügend großer Wahrscheinlichkeit nicht geraten werden können. Dies bedeutet beispielsweise, dass gewählte Passwörter in keinem Lexikon zu finden sein sollten, über eine angemessene Anzahl von Passwortzeichen verfügen sollten und nach Möglichkeit auch Zeichen wie Ziffern oder Sonderzeichen enthalten sollten. Was sich jedoch positiv auf die Sicherheit auswirkt, stellt in der Praxis ein Problem für den Menschen dar: Er kann sich solche Passwörter nur sehr schlecht merken. Die Situation spitzt sich durch die immer größer werdende Anzahl von Passwörtern zu, die sich Computernutzer merken müssen. Dies wird darüber hinaus sogar noch weiter erschwert, da einige Unternehmen und Internet-Dienste Mitarbeiter bzw. Benutzer auffordern, ihre Passwörter in bestimmten zeitlichen Abständen zu verändern. Um diese Situation bewältigen zu können, verwenden viele Computernutzer bei unterschiedlichen Diensten bzw. Anwendungen das gleiche Passwort, was wiederum Sicherheitsprobleme mit sich bringt. Wenn Computernutzer hingegen zu viele unterschiedliche Passwörter haben, die sie sich



nicht merken können, dann notieren sie diese; leider werden die Notizen dann oftmals an leicht zugänglichen Orten hinterlegt, so dass andere leicht an diese Passwörter gelangen können.

Sicherheitsbewusstere Computernutzer speichern heutzutage ihre Passwörter oftmals verschlüsselt auf ihrem Computer oder USB-Sticks ab, jedoch hat dies den Nachteil, dass Passwörter nur dann verfügbar sind, wenn der Computernutzer auch Zugriff auf die entsprechende Hardware hat. In Internet-Cafés oder an anderen fremden Computern besteht bei einer lokalen Speicherung leider kein Zugriff auf die Passwörter. Bei Verwendung von USB-Sticks braucht man als Nutzer die Erlaubnis des Computerbesitzers, um diesen an den Computer anschließen zu können, was aus Sicherheitsgründen oftmals abgelehnt wird. Darüber hinaus hat die Speicherung von Passwörtern auf einem Computer —ob verschlüsselt oder unverschlüsselt— einen Nachteil, wenn Computernutzer typischerweise mit mehreren Endgeräten arbeiten, wie z.B. einem Desktop-Computer im Büro, einem Notebook unterwegs und einem anderen Desktop-Computer zu Hause —möglicherweise am Telearbeitsplatz—, da in diesem Fall die gespeicherten Passwortdaten zwischen den Endgeräten synchronisiert werden müssen. Die Alternative mit einer auf einen Server ausgelagerten Speicherung von Passwortdaten verlangt hingegen, dass der Server auf jedem Fall verfügbar ist. Sind die Passwortdaten unverschlüsselt auf dem Server abgelegt, dann können diese von dem Betreiber des Server-Dienstes missbraucht werden, selbst wenn der Server gegenüber Zugriffen aus dem Internet über eine wirksame Zugriffskontrolle verfügt. Legt man Passwortdaten auf dem Server verschlüsselt ab —beispielsweise in Form einer verschlüsselten Datei—, und gelangen diese verschlüsselten Daten in die Hände eines Angreifers, dann kann dieser immerhin eine Offline-Attacke durchführen, indem er versucht —ob mittels vollständiger Suche oder in intelligenterer Weise— die Daten zu entschlüsseln.

Die Probleme, die sich rund um die Verwendung von Passwörtern ergeben, wurden bereits in einer Reihe von Studien quantitativ ermittelt. Als Beispiel sei hier die SafeNet-Studie¹ aus dem Jahr 2004 genannt, aus welcher hier einige Ergebnisse angeführt werden sollen:

- 😊 50% der befragten Computernutzer schreiben ihre Passwörter auf und hinterlegen entsprechende Zettel am Arbeitsplatz.
- 😊 Mehr als 33% der befragten Computernutzer haben ihre Passwörter Arbeitskollegen mitgeteilt.
- 😊 67% der Computernutzer verwenden mindestens 5 Dienste oder Anwendungen, für welche sie ein Passwort benötigen.
- 😊 47% der Computernutzer verwenden Dienste oder Anwendungen, bei denen das Passwort mindestens einmal im Jahr geändert werden muss.
- 😊 68% der befragten Unternehmen haben spezielle Anforderungen an die auszuwählenden Passwörter (z.B. geforderte Mindestlänge und Verwendung von Sonderzeichen in Passwörtern).

¹ SafeNet: 2004 Annual Password Survey Results. March 2005, www.safenet-inc.com



Je nach Kontext des Passwortheinsatzes —ob privat oder professionell— können die typischen Probleme des Passwort-Managements deutlich unterschiedliche Konsequenzen haben. Während ein im privaten Kontext vergessenes Passwort für den Computernutzer eher nur als lästig oder unerwünscht einzustufen ist, so können ihm bei schwach gewählten Passwörtern und darauf ansetzenden Angriffen weitere Konsequenzen drohen, wie beispielsweise durch Verlust der Privatsphäre und Identitätsdiebstahl oder auch direkte finanzielle Verluste durch Initiierung und Manipulation von Transaktionen im Rahmen des elektronischen Handels wie etwa bei Online-Auktionen. Im professionellen Kontext können die Probleme des Passwort-Managements zu weiteren negativen Konsequenzen führen. Vergessene Passwörter führen zu Helpdesk-Kosten und beeinflussen die Produktivität des jeweiligen Mitarbeiters, da dieser vorübergehend die gewünschte Anwendung nicht benutzen kann und so lange warten muss, bis sein Passwort zurückgesetzt worden ist. Nach Forrester Research belaufen sich die durch Passwort-Probleme hervorgerufenen Helpdesk-Kosten in Unternehmen im Durchschnitt auf ungefähr 200 US-Dollar pro Mitarbeiter und Jahr. Schwach gewählte Passwörter bergen für Unternehmen das Risiko, dass geheime Informationen an die Öffentlichkeit oder in die Hände von Konkurrenten gelangen können oder dass Unternehmensdaten manipuliert bzw. gelöscht werden können. Diese Risiken sind für Unternehmen vor dem Eintreten von Schadensfällen schwierig zu quantifizieren und leider in der heutigen Praxis auch nicht zu kontrollieren. Als Unternehmen hat man heutzutage keine Kontrolle darüber, ob Angestellte ihre Passwörter, welche diese für berufliche Zwecke verwenden, auch im privaten Kontext einsetzen. Gerät ein solches Passwort über den Gebrauch im privaten Kontext in die falschen Hände, dann kann es für Angreifer ein leichtes Spiel sein, an vertrauliche Unternehmensdaten zu gelangen. Selbst wenn es für die private Wiederverwendung beruflich genutzter Passwörter heute keine verfügbaren Datenerhebungen gibt, so ist doch anzunehmen, dass viele Arbeitnehmer ihre beruflich genutzten Passwörter beispielsweise auch zur Anmeldung bei privat genutzten Online Communities oder anderen Zwecken verwenden.

Dies und viele andere Probleme lassen sich bei der Verwendung des PasswordSitters vermeiden. Das sich für ein Unternehmen durch die Nutzung des PasswordSitters ergebende Einsparpotenzial hängt direkt vom unternehmensspezifischen Risiko ab, d.h. von dem Wert der jeweiligen Daten für das Unternehmen. Bei einer Gesamtkostenbetrachtung sind für ein Unternehmen die mit dem Sicherheitsrisiko in Beziehung stehenden Kosten nochmals zu den Helpdesk-Kosten und dem Produktivitätsausfall zu addieren. Ein Unternehmen kann selbst dann noch deutlich Kosten einsparen, wenn die in einem Jahr pro Mitarbeiter durchschnittlich anfallenden Helpdesk-Kosten sich nur auf einen Bruchteil der von Forrester Research angegebenen Helpdesk-Kosten belaufen. Ebenso bringt der PasswordSitter im privaten Anwendungsbereich Vorteile. Man muss sich als Computernutzer nur noch ein Master-Passwort merken, und dennoch sind alle Passwörter genügend sicher und für den Benutzer von jedem Endgerät aus verfügbar, sogar auf einem Computer in einem Internet-Café an einem beliebigen Ort der Welt; und dies, ohne dass die Passwörter an irgendeiner Stelle gespeichert werden. Darüber hinaus sind alle dienst- und anwendungsspezifischen Passwörter unterschiedlich, d.h. Unternehmen müssen keine Sorgen mehr haben, dass ihre Mitarbeiter beruflich verwendete Passwörter auch im privaten Kontext bei verschiedenen Internet-Diensten verwenden und damit bis dahin kaum kontrollierbare Risiken für das Unternehmen verursachen. Nicht verfügbare Passwörter gehören der Vergangenheit an, ohne Mühen für Speichern, Ausdrucken oder Notieren. So lange der Computernutzer sein Master-Passwort geheim hält, bleiben alle Passwörter sicher.



Die Alternativen

Grundsätzlich bieten sich zwei Strategien zur Verbesserung der heutigen Situation im Bereich der Authentifizierung von Benutzern an: Entweder man setzt neue technische Verfahren zur Authentifizierung ein oder man verwendet weiterhin den Passwortmechanismus und bietet gleichzeitig Lösungen zum besseren, sichereren und benutzerfreundlicheren Management von Passwörtern an.

Die mit großem Abstand meisten Angebote im World Wide Web setzen Passwortverfahren ein, auch wenn es einige andere technische Verfahren zur Authentifizierung gibt, wie beispielsweise der Einsatz von PKI-basierten Verfahren. Würde ein Anbieter jedoch von seinen Kunden verlangen, dass sie sich für zukünftige Authentifizierungsvorgänge ein entsprechendes Schlüsselpaar mit Zertifikat besorgen, dann könnte man davon ausgehen, dass dieser wegen der damit einhergehenden Kosten und Aufwände den Großteil seiner Kunden verlieren würde.

Andere Alternativen wie Einmalpasswörter bieten ebenfalls ein geeignet hohes Sicherheitsniveau, jedoch ist ihr Einsatz hauptsächlich einigen wenigen Bereichen vorbehalten, wie beispielsweise den Bankanwendungen. Darüber hinaus kann man bei einem mobilen Benutzer Computernutzer nicht davon ausgehen, dass dieser ständig seine Einmalpasswörter verfügbar hat.

Andere Ansätze, die in Richtung web-basierter Single Sign-on (SSO) Dienste auf Basis von föderierten Identitäten gehen wie beispielsweise die Aktivitäten der Liberty Alliance, sind noch nicht in der Praxis verfügbar. Darüber hinaus erfordern sie den Aufbau einer entsprechenden Infrastruktur und sind mit Investitionen für Anbieter verbunden. Selbst wenn diese Systeme in Zukunft verfügbar sein werden, dann ist anzunehmen, dass sich nicht sämtliche Betreiber von Diensten, welche man als Computernutzer verwendet, zu Identitätsföderationen zusammenschließen werden. Insbesondere von kleineren Anbietern ist zu erwarten, dass diese nicht in die Föderationskonzepte größerer Akteure einbezogen werden. Es ist also anzunehmen, dass sich Computernutzer weiterhin bei diesen mittels Passwortverfahren anmelden werden, selbst wenn SSO-Lösungen auf Basis von föderierten Identitäten verfügbar sein werden. Vor diesem Hintergrund bietet der PasswordSitter eine sinnvolle und wertvolle Ergänzung zu zukünftigen SSO-Lösungen auf Basis von föderierten Identitäten an. Er gewährleistet, dass man als Computernutzer jederzeit sicher und benutzerfreundlich identifizieren kann, auch wenn Dienstanbieter keine föderierten Identitäten unterstützen.

Die Einführung von SSO-Systemen in Unternehmensnetzen stellt ebenfalls eine Möglichkeit dar, die Authentifizierung für den Computernutzer einfacher zu machen. SSO-Systeme haben jedoch den Nachteil, dass jede Anwendung, welche SSO-fähig sein soll, entsprechend modifiziert werden muss, damit der Authentifizierungsvorgang vereinfacht wird und man als Computernutzer nicht für jede Anwendung ein Passwort eingeben muss und sich diese nicht mehr merken muss. Die Umstellung zum SSO-fähigen Betrieb ist jedoch aufwändig und sie muss für jede bestehende Anwendung wie auch jede zukünftige Anwendung geleistet werden, sofern sie überhaupt möglich ist. Es ist anzunehmen, dass in einem Unternehmen wahrscheinlich nicht sämtliche Anwendungen, welche Passwörter benötigen, entsprechend SSO-fähig gemacht werden können, so dass es immer noch Systeme geben wird, für welche klassische Passwortverfahren verwendet werden müssen. Selbst wenn also ein Unternehmen SSO-Systeme einsetzt, kann der PasswordSitter eine sinnvolle Ergänzung bieten.



Wenngleich sich in der Praxis eine Reihe von Problemen beim Management von Passwörtern ergeben, so sind Passwortverfahren immer noch die am stärksten verbreiteten Verfahren zur Authentifizierung von Benutzern —und werden es wahrscheinlich auch auf absehbare Zeit hin bleiben. Vor diesem Hintergrund bietet es sich an, durch neue technische Lösungen zur Beseitigung der heute existierenden Probleme beim Management von Passwörtern beizutragen. Zur Umsetzung dieser Strategie bietet sich der PasswordSitter an.

Funktionsweise des PasswordSitters

Der PasswordSitter basiert auf einem bei Fraunhofer SIT entwickelten Verfahren, welches dem Patentamt zur Patentierung vorliegt. Ziel des Verfahrens ist es, ausgehend von einem geheimen Master-Passwort und anderen Parametern, die nicht geheim gehalten werden müssen, im Bedarfsfall das jeweilige Dienst- bzw. Anwendungspasswort eines Benutzers zu berechnen und dem Computernutzer zur Verfügung zu stellen. Zu diesen genannten Parametern gehören die Identität des Computernutzers bei dem betrachteten Dienst bzw. der betrachteten Anwendung, eine Bezeichnung für den Dienst bzw. die Anwendung und die Passwortregeln, um die Anforderungen des Dienstes bzw. der Anwendung hinsichtlich Passwortheigenschaften wie beispielsweise Passwortlänge oder erforderliche Zeichentypen zu erfüllen. Optional kann als Parameter auch eine zusätzliche Versionsangabe verwendet werden, welche zum Wechsel von Passwörtern —z.B. monatlich oder jährlich— hilfreich ist.

Bei dem Verfahren werden die Identität des Computernutzers, die Dienst- bzw. Anwendungsbezeichnung und die optionale Versionsangabe mit dem Verschlüsselungsverfahren AES verschlüsselt. Bei AES handelt es sich um ein weltweit standardisiertes und von Experten als sicher bewertetes Verschlüsselungsverfahren. Der hierzu verwendete Schlüssel wird aus dem Master-Passwort berechnet. Aus dem Ergebnis der Verschlüsselung wird durch Berücksichtigung der Passwortregeln das jeweilige Passwort konstruiert. Die somit erzeugten Passwörter entsprechen den Anforderungen an starke Passwörter. Wenn die interne Berechnungsfunktion des PasswordSitters das Passwort der jeweiligen Anwendung berechnet hat, kann dieses im nächsten Schritt an die Anwendung übergeben werden. Dies wird in Abbildung 1 gezeigt.

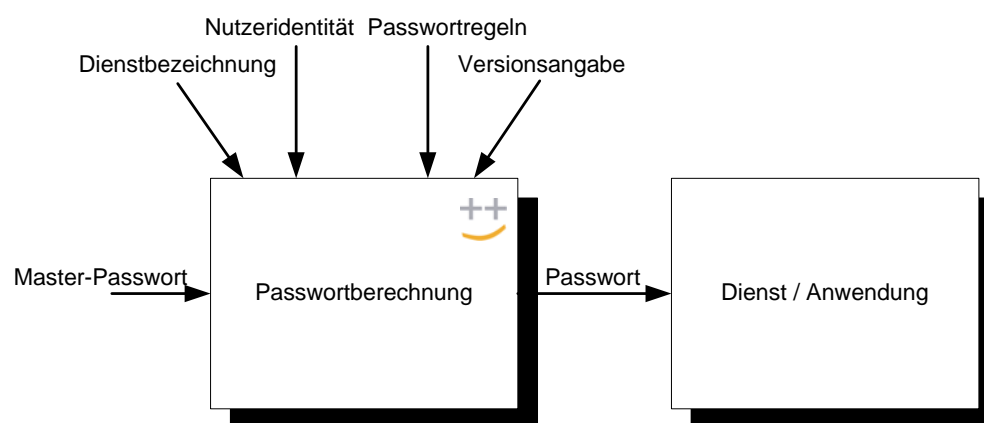


Abbildung 1: Die Passwortberechnung im PasswordSitter



Zur benutzerfreundlichen Bedienung kann man den PasswordSitter in zwei verschiedenen Modi verwenden. In einem Online-Modus und einem Offline-Modus, wobei es im Offline-Modus nochmals zwei Subvarianten gibt.

Damit ein Computernutzer an verschiedenen Endgeräten seine Passwörter erzeugen kann und hierzu nicht jeweils seine dienst- bzw. anwendungsspezifischen Parameter (Nutzeridentität, Dienstbezeichnung, Versionsangabe, Passwortregeln) angeben muss, kann er diese auf einem Server ablegen, von wo aus diese dann im Bedarfsfall zur Passwortberechnung geladen werden können, wie in Abbildung 2 gezeigt wird. Auf diesem Server können Benutzer die Parameter für unterschiedliche Dienste bzw. Anwendungen ablegen.

Die Gesamtheit der von einem Benutzer abgelegten Parameter wird hier als Benutzerprofil bezeichnet. Jeder Benutzer erhält ausschließlich Zugang zu seinem eigenem Profil. Der Zugang ist passwortgeschützt, jedoch muss der Computernutzer sich hierfür kein eigenes Passwort merken. Das Server-Passwort wird aus dem Master-Passwort derart berechnet, dass sowohl der Anbieter des Servers wie auch jeder Angreifer, der sich in irgendeiner Weise Zugang zu dem Server-Passwort verschafft, nicht auf das Master-Passwort zurück schließen können. Wenn der Computernutzer sein Master-Passwort ändert, dann ändert sich ebenfalls das Server-Passwort.

Die Variante, in welcher der Computernutzer zur Berechnung seiner Passwörter Server-Dienste in Anspruch nimmt, wird als Online-Modus bezeichnet. Es wird an dieser Stelle nochmals ausdrücklich darauf hingewiesen, dass das Master-Passwort zu keinem Zeitpunkt an den Server übertragen wird. Sogar in einem Fall, in welchem es einem Angreifer gelingen würde, in den Server eindringen und diesen zu übernehmen, könnte der Angreifer die Passwörter der Computernutzer nicht in Erfahrung bringen.

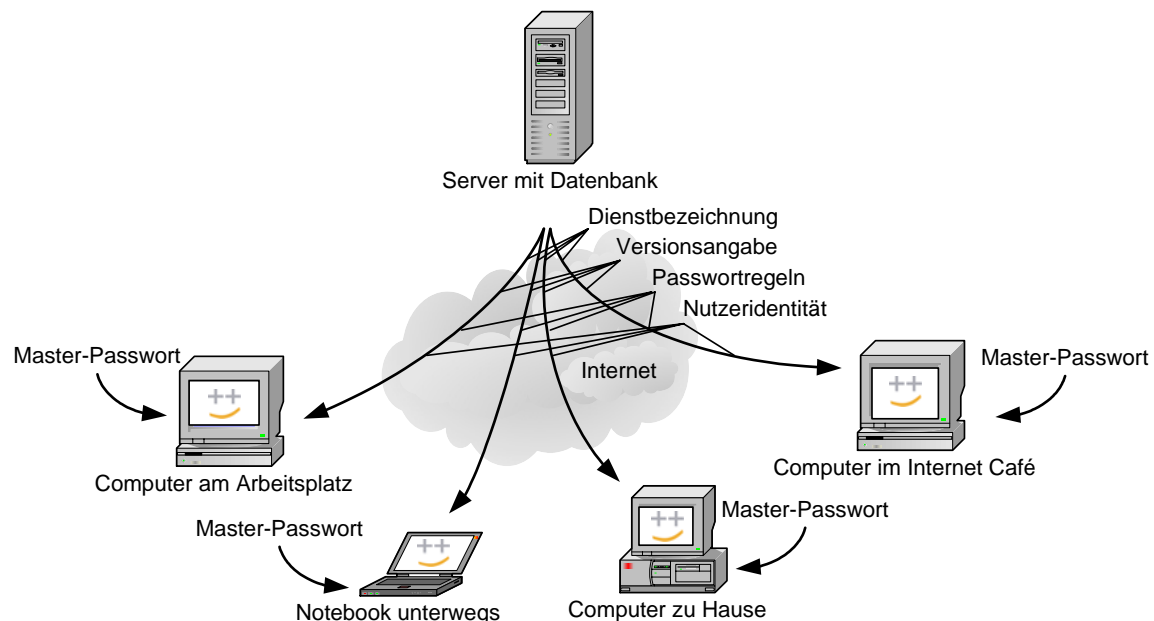


Abbildung 2: Der PasswordSitter im Online-Modus

Der Offline-Modus zeichnet sich dadurch aus, dass die zur Passwortberechnung benötigten Daten nicht vom Server bereitgestellt werden. Der PasswordSitter unterstützt zwei Varianten des Offline-Modus.



In der ersten Variante des Offline-Modus hat sich der Computernutzer im Vorfeld sein Profil von dem Server auf seinen Computer herunter geladen und mit dem PasswordSitter in eine Datei exportiert. Diese Datei speichert der Benutzer auf seinem Computer ab. In dieser Datei befindet sich dann das komplette Profil des Benutzers. Aus Sicherheitsgründen kann das lokale Profil verschlüsselt gespeichert werden. Zur Verschlüsselung wird wiederum das AES-Verfahren angewendet, wobei als Schlüssel ein aus dem Master-Passwort berechnetes Geheimnis dient. Möchte der Computernutzer an einem seiner Endgeräte eine Anwendung starten, für die er ein Passwort benötigt, dann kann er hierzu das lokal abgelegte Profil verwenden.

Der Computernutzer muss in dieser Variante des Offline-Modus nur sein Master-Passwort in den PasswordSitter eingeben. Der PasswordSitter liest die verschlüsselte Profildatei ein, entschlüsselt sie mit dem aus dem Master-Passwort berechneten Schlüssel und stellt das Profil für den Computernutzer dar. Wählt dieser in seinem Profil den gewünschten Dienst bzw. die gewünschte Anwendung aus, dann berechnet der PasswordSitter das entsprechende Passwort.

In dieser Variante des Offline-Modus wird davon ausgegangen, dass der Computernutzer sein Passwort auf einem solchen Endgerät berechnet, auf welchem er seine Profildaten vorher exportieren konnte. Der Vorgang wird in Abbildung 3 gezeigt.

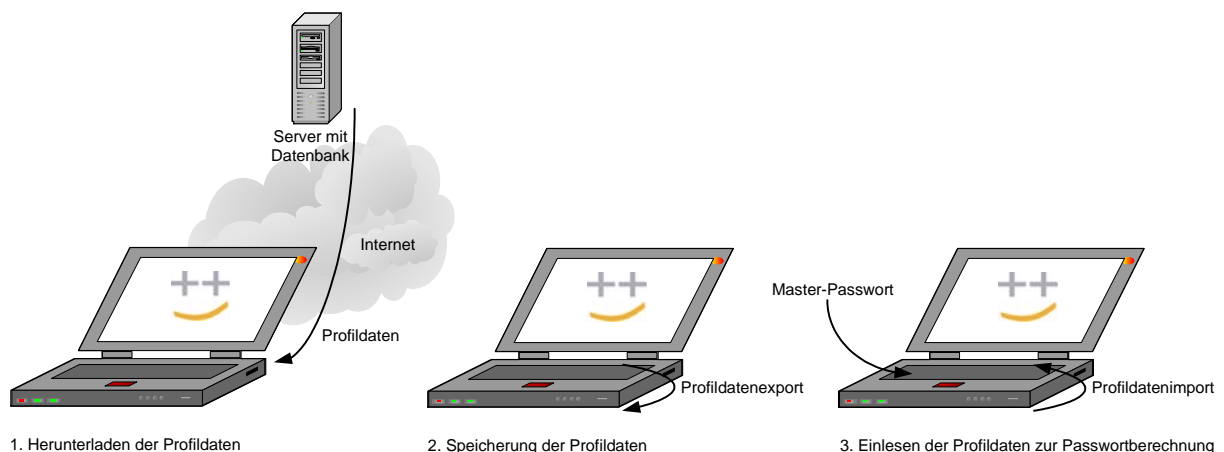


Abbildung 3: Passwortberechnung im Offline-Modus mit lokal gespeicherten Profildaten

Die oben beschriebene Variante des Offline-Modus, bei welcher auf lokal gespeicherte Profildaten zurückgegriffen wird, ist in der Praxis nicht immer anwendbar. Man betrachte beispielsweise den Fall, in welchem der Computernutzer an einem fremden Computer seine Emails lesen möchte. Da auf einem fremden Computer die eigenen Profildaten nicht verfügbar sind, muss man diese zur Passwortberechnung nun per Hand eingeben. Dies bedeutet, dass er außer dem Master-Passwort zusätzlich noch seine Nutzeridentität, die entsprechende Dienstbezeichnung, eine Versionsangabe (sofern erforderlich) und die jeweiligen Passwortregeln einzugeben sind, wie in Abbildung 4 gezeigt wird. Aus Gründen der Benutzerfreundlichkeit sind die Möglichkeiten zur Einstellung von Passwortregeln sehr reduziert. Die Strategie des PasswordSitters ist es dabei, die von einem Dienst bzw. einer Anwendung vorgegebenen Passwortregeln nicht exakt abzubilden, sondern stattdessen eigene Regeln für die Generierung der Passwörter anzugeben, die sich an den vorgegebenen Passwortregeln orientieren. Mit den so im PasswordSitter einstellbaren Passwortregeln kann erreicht werden, dass die mit entsprechenden Vorgaben erzeugbaren Passwörter auf jeden Fall die vorgegebenen



Passwortregeln erfüllen, auch wenn möglicherweise nicht alle zu den Regeln eines Dienstes bzw. einer Anwendung konformen Passwörter von dem PasswordSitter erzeugt werden können, wie in Abbildung 5 gezeigt wird. Dennoch sind aus Sicherheitsgründen die jeweiligen Mengen der mit dem PasswordSitter generierbaren Passwörter groß genug, so dass eine erfolgreiche vollständige Suche ausgeschlossen werden kann. Durch diesen beim PasswordSitter gewählten Ansatz gelingt es, mit sehr wenigen Einstellungen, die vom Benutzer in dieser Variante des Offline-Modus vorgenommen werden müssen, dienst- bzw. anwendungskonforme Passwörter zu erzeugen.

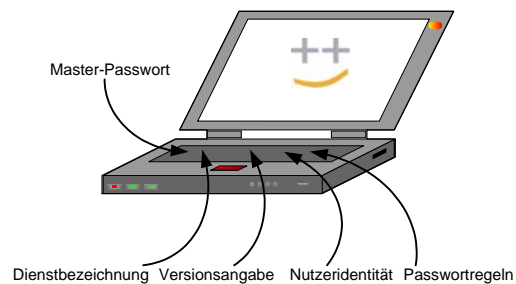


Abbildung 4: Passwortberechnung im Offline-Modus mit Eingabe der Profildaten per Hand

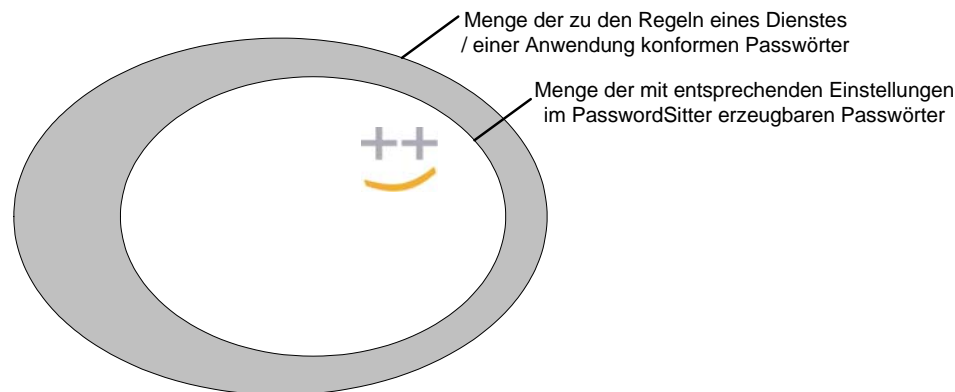


Abbildung 5: Mengen der regelkonformen und der erzeugbaren Passwörter

Nachdem der PasswordSitter ein Passwort berechnet hat, legt er dieses in der Zwischenablage des Computers ab. Dies erlaubt es dem Computernutzer, das Passwort benutzerfreundlich in das Anmeldefeld des jeweiligen Dienstes bzw. der Anwendung zu übertragen. Nach einer kurzen Zeit, z.B. 60 Sekunden, löscht der PasswordSitter das Passwort wieder aus der Zwischenablage, um Missbrauchsmöglichkeiten auszuschließen, z.B. durch andere Personen, welche die Zwischenablage des Computers zu einem späteren Zeitpunkt auslesen können.

Den PasswordSitter gibt es in zwei verschiedenen Implementierungsformen. Als Computernutzer kann man ihn sowohl als Applikation als auch als signiertes Java-Applet einsetzen. Die Applikation wird auf dem eigenen Computer installiert. Das signierte Applet wird im Bedarfsfall über das Internet geladen. Die Bereitstellung der Funktionalität als herunterladbares und signiertes Applet ist insbesondere in dem Fall hilfreich, wenn ein Benutzer an einem fremden Computer sein Passwort benötigt. Sofern ein Internetzugang zur Verfügung steht, kann der Benutzer den PasswordSitter von einer vertrauenswürdigen Stelle herunterladen. Die Tatsache, dass es sich um ein signiertes Applet handelt, versichert den Benutzer dahingehend, dass er sein Master-Passwort nicht einer manipulierten Software übergibt. In beiden



Implementierungsformen wird die Passwortgenerierung in exakt der gleichen Weise durchgeführt, so dass man als Computernutzer situationsabhängig sowohl mit der Applikations- als auch mit der Applet-Variante arbeiten kann.

Der PasswordSitter in der Praxis

Im Folgenden wird kurz demonstriert, wie man den PasswordSitter bedient. Wenn man als Computernutzer eines seiner Passwörter benötigt, dann startet man zunächst den PasswordSitter. Diesen kann man entweder als signiertes Applet von einer Seite laden, die den PasswordSitter anbietet, oder der PasswordSitter ist bereits auf dem verwendeten Computer installiert und kann direkt von dort aus gestartet werden. Die Bedienung von beiden Implementierungsformen geschieht in identischer Weise.

Möchte man an einem fremden Computer an seine Passwörter gelangen, dann wird man wahrscheinlich auf die Variante zurückgreifen, bei welcher der PasswordSitter als signiertes Applet von dem Web-Server geladen wird. Nachdem der PasswordSitter geladen und gestartet ist, zeigt sich ein Anmeldefenster, welches in Abbildung 6 dargestellt ist. In dem hier gezeigten Beispiel wird der PasswordSitter von der Adresse <https://www.password-sitter.de> geladen.

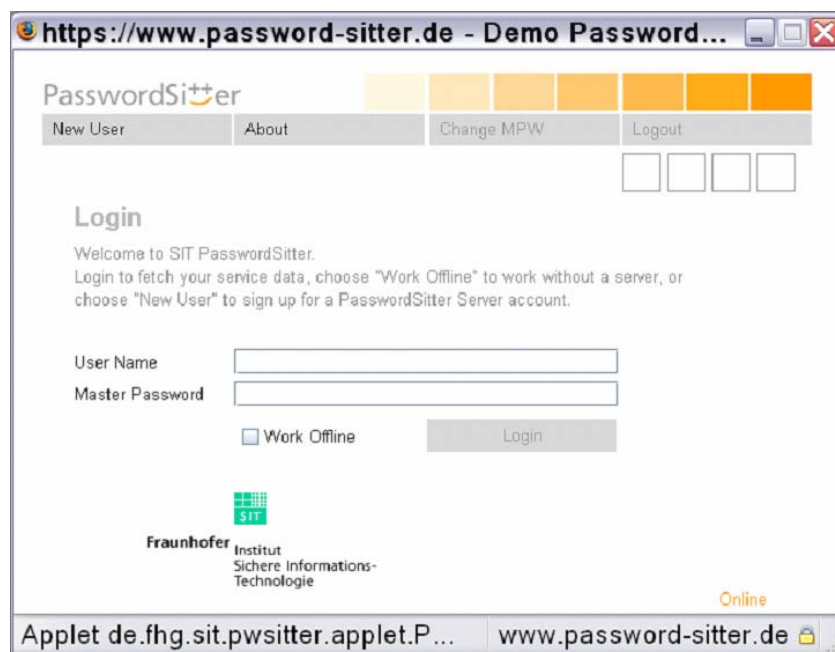


Abbildung 6: Das Anmeldefenster des PasswordSitters

Als Computernutzer kann man sich nun entscheiden, ob man den PasswordSitter im Online- oder Offline Modus benutzen möchte. An dieser Stelle sei zunächst der Online-Modus betrachtet.

Im Online-Modus lädt der PasswordSitter das Profil des Benutzers von einer Datenbank. Wir nehmen an, dass man sich als Computernutzer bereits bei dem zugehörigen Datenbank-Dienst angemeldet hat und dort über ein Zugangskonto verfügt. Um sich bei der Datenbank anzumelden, gibt man als Computernutzer seinen Namen und das Master-Passwort ein. Es sei an dieser Stelle nochmals ausdrücklich darauf hingewiesen, dass das Master-Passwort in dem



PasswordSitter verbleibt und nicht zur Anmeldung an die Datenbank geschickt wird. Stattdessen berechnet der PasswordSitter aus dem Master-Passwort ein Datenbank-Passwort, aus welchem der Datenbank-Betreiber nicht auf das Master-Passwort zurück schließen kann.

In dem in Abbildung 7 gezeigten Beispiel gibt der Computernutzer seine Datenbank-Identität „MagisterLudi“ und sein Master-Passwort ein. Nach Eingabe des vollständigen Master-Passworts berechnet der PasswordSitter eine optische Rückmeldung—in Abbildung 7 ein schwarzes Dreieck auf rotem Hintergrund—, welches dem Computernutzer signalisiert, ob er sein Master-Passwort richtig eingegeben hat oder ob sich möglicherweise Tippfehler eingeschlichen haben. Im Vergleich zu der Anzahl der Master-Passwörter gibt es sehr viel weniger verschiedene Symbol-/Farb-/Positionskombinationen, d.h. mehrere Kandidaten von unterschiedlichen Master-Passwörtern führen zur Anzeige der gleichen optischen Rückmeldung. Die Darstellung der optischen Rückmeldung ist unbedenklich, selbst wenn auch andere Personen den Computerbildschirm und damit das angezeigte Symbol sehen können. Aus der optischen Rückmeldung kann man nicht auf das Master-Passwort zurück schließen. Die optische Rückmeldung ist insbesondere für den später gezeigten Offline-Modus hilfreich. Damit die optische Rückmeldung dem Computernutzer im Offline-Modus helfen kann, ist es von Vorteil, wenn sie auch im hier betrachteten Online-Modus angezeigt wird.



Abbildung 7: Die Anmeldung bei der Datenbank im Online-Modus und optische Rückmeldung

Nachdem man sich bei der Datenbank erfolgreich angemeldet hat, lädt der PasswordSitter das Profil aus der Datenbank. Das Profil zeigt sämtliche Dienste und Anwendungen an, für welchen der PasswordSitter die jeweiligen Passwörter verwalten soll. In dem in Abbildung 8 dargestellten Beispiel sind dies die Passwörter des Computernutzers für die Dienste

++ GMX

++ Secure Service



++ Planet

++ WorldGate.

Die Liste der im Profil enthaltenen Dienste und Anwendungen kann beliebig lang sein, so dass man beliebig viele Passwörter mit dem PasswordSitter verwalten kann. Auf die Verwaltung des eigenen Profils wird an späterer Stelle eingegangen. Darüber hinaus zeigt der PasswordSitter an, wann der letzte erfolgreiche oder auch abgelehnte Anmeldeversuch bei der Datenbank stattgefunden hat. Die optische Rückmeldung (hier das schwarze Dreieck auf rotem Hintergrund) wird weiterhin angezeigt, so lange der Computernutzer eingeloggt ist.

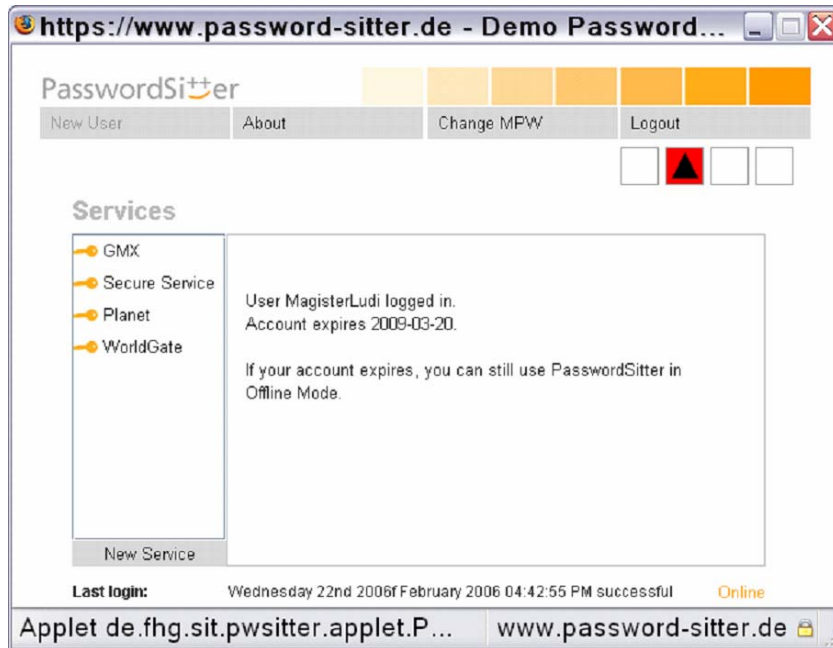


Abbildung 8: Das aus der Datenbank geladene Profil

Wählt der Computernutzer per Mausklick einen Dienst aus dem Profil aus, dann werden ihm die für diesen Dienst relevanten Daten wie Login-Name für diesen Dienst und die eingestellten Regeln zur Passwortgenerierung angezeigt. Darüber hinaus wird das Passwort für den Dienst berechnet und für einige Sekunden (z.B. 60 Sekunden) in die Zwischenablage gelegt, so dass es bequem in das Anmeldeformular des Dienstes kopiert werden kann.



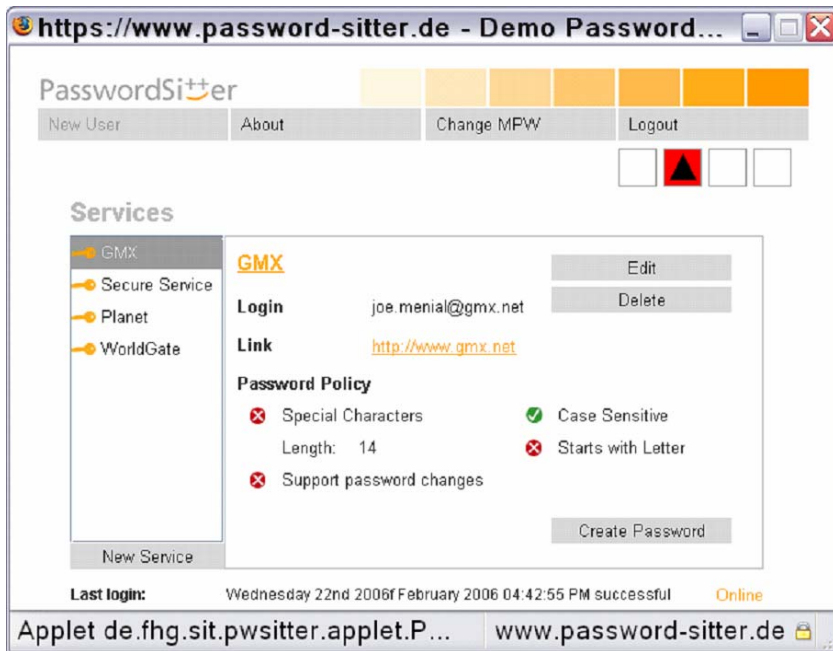


Abbildung 9: Die Profildaten eines einzelnen Dienstes

Die Anzeige der Profildaten inklusive Passwortregeln für einen Dienst ist sinnvoll, damit ein Benutzer sich in dem Fall des Offline-Betriebs, bei dem er sämtliche Parameter von Hand eingeben muss, besser an diese erinnern kann. Die angezeigte Option „Create Password“ dient für den Fall, dass das berechnete Passwort wegen Zeitüberschreitung bereits schon wieder aus der Zwischenablage gelöscht wurde. Durch Anklicken dieser Option wird das Passwort nochmals für einige Sekunden in die Zwischenablage gelegt.



Abbildung 10: Die Profildaten für den Dienst „Secure Service“



Möchte man sich bei einem anderen Dienst anmelden, dann muss man sich lediglich aus der links gezeigten Liste den jeweiligen Dienst auswählen. Dadurch wird das Passwort für den neu ausgewählten Dienst erzeugt und in der Zwischenablage abgelegt. Ist in der Zwischenablage noch ein vorher berechnetes Passwort vorhanden, dann wird dieses durch das neu berechnete Passwort überschrieben. In Abbildung 10 wählt sich der Computernutzer den (Dummy-)Dienst „Secure Service“ aus. Neben der im Hintergrund erfolgenden Berechnung des Passworts für diesen Dienst zeigt der PasswordSitter die Profildaten des Dienstes an. Die Passwortberechnung folgt den angegebenen Passwortregeln: Sonderzeichen erforderlich, Unterscheidung von Groß- und Kleinbuchstaben, Passwortlänge 16, erstes Zeichen nicht zwingend Buchstabe, keine Unterstützung von Passwortwechseln (keine Versionierung von Passwörtern eingestellt).

Das vom PasswordSitter berechnete Passwort für „Secure Service“ kann nun bequem über die Zwischenablage in das Anmeldeformular eingegeben werden. Neben dem Passwort kann auch der Login-Name des Computernutzers über die Zwischenablage in das Anmeldeformular übertragen werden. Der Anmeldevorgang bei „Secure Service“ wird in Abbildung 11 gezeigt.

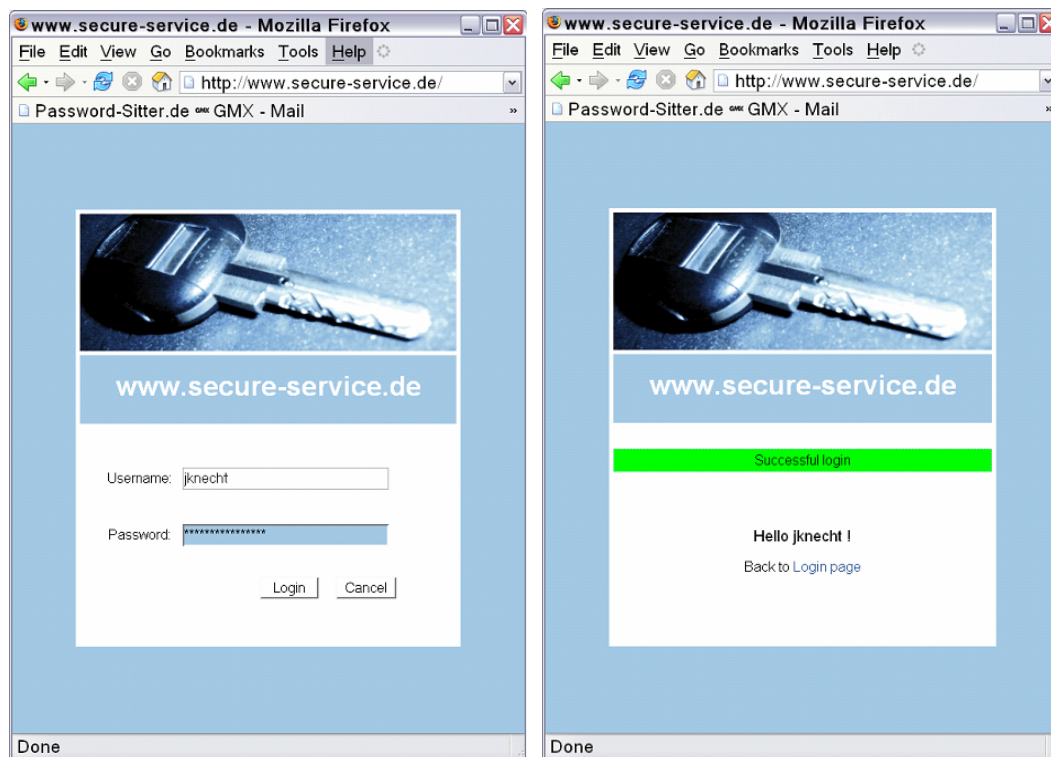


Abbildung 11: Anmeldung bei Secure Service

Das vom PasswordSitter für „Secure Service“ berechnete Passwort wird in Abbildung 12 gezeigt. Hier wurde es anstatt in ein Anmeldeformular über die Zwischenablage in einen Editor übertragen. Die Einhaltung der in Abbildung 10 gezeigten Passwortregeln kann leicht überprüft werden.





Abbildung 12: Passwort für Secure Service

Registriert man sich bei einem neuen Dienst, zu dessen Zugang man ein Passwort benötigt und welches man mit dem PasswordSitter verwalten möchte, dann ergänzt man das vorhandene Profil um einen neuen Eintrag. Um dies zu initiieren wählt man in der Dienstliste die Option „New Service“ aus, die beispielsweise in Abbildung 8, Abbildung 9 oder Abbildung 10 gezeigt wird. Danach öffnet sich im PasswordSitter ein Fenster, in das man die Profildaten für einen neuen Dienst einträgt. Wenn man die Daten eingetragen hat, werden diese zur Datenbank übertragen und abgespeichert. Abbildung 13 zeigt die Anlegung eines neuen Dienstes „My New Service“, bei welchem Login-Name „MyLogin“, die erforderlichen Passwortregeln und die Versionsangabe eingegeben werden. Die Versionsangabe —in Abbildung 13 „Mar“ und „06“— erlaubt die Änderung der Passwörter, ohne dass das Master-Passwort verändert werden muss. Durch Anklicken der Option „Create“ werden die Profildaten von „My New Service“ an die Datenbank übertragen und abgespeichert. Von dort können die Profildaten bei Bedarf geladen werden, um das Passwort für „My New Service“ zu berechnen.

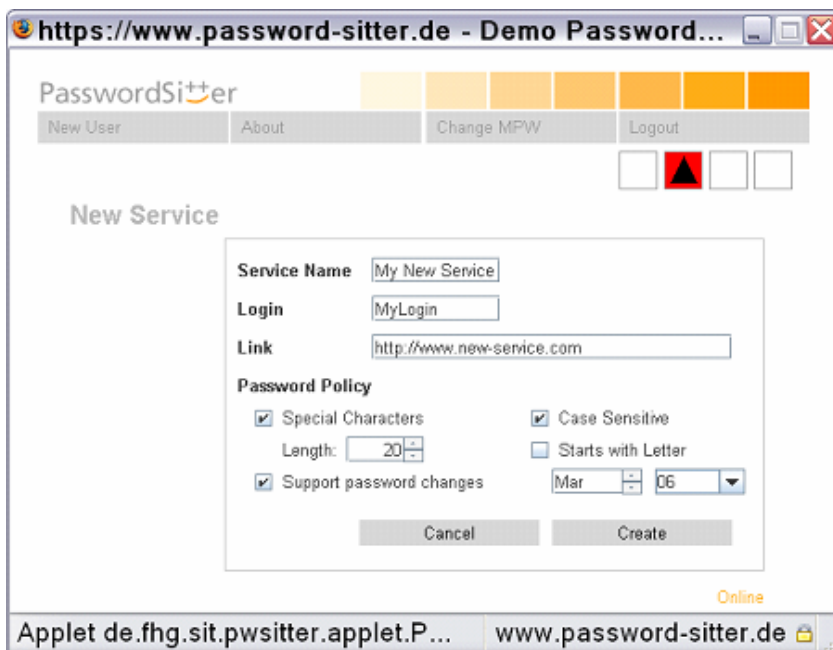


Abbildung 13: Die Anlegung eines neuen Dienstes „My New Service“ im PasswordSitter

Der PasswordSitter unterstützt Computernutzer bei der Änderung von Passwörtern. Dies kann beispielsweise erforderlich sein, wenn Passwörter für bestimmte Dienste in regelmäßigen zeitlichen Abständen geändert werden müssen. Die Berechnung des Passwortes für den Dienst „WorldGate“ hängt, wie in Abbildung 14 gezeigt wird, von der Versionsangabe „Feb 06“ ab. Soll das Passwort für „WorldGate“ geändert werden, ohne dass das Master-Passwort verändert werden soll, dann wählt man bei den Profildaten von „WorldGate“ die Option „Edit“. Danach



erlaubt der PasswordSitter die in Abbildung 15 gezeigten Profildaten zu verändern. Ändert man als Computernutzer die Versionsangabe von „Feb 06“ zu „Mar 06“ wie in Abbildung 16 gezeigt und speichert die neue Einstellung durch Anklicken der Option „Save“ in der Datenbank, dann unterstützt der PasswordSitter die Umstellung des Dienstpassworts.



Abbildung 14: Die Profildaten des Dienstes WorldGate



Abbildung 15: Zu verändernde Profildaten bei WorldGate

Typischerweise muss man bei einem Passwortwechsel bei einem Dienst zunächst das alte Passwort und danach zweimal das neue Passwort eingeben. Wenn die neue Versionsangabe in



der Datenbank gespeichert wurde, dann erlaubt der PasswordSitter dem Computernutzer, das alte und das neue Passwort nacheinander in die Zwischenablage zu kopieren, wie in Abbildung 17 dargestellt wird. Die hier gezeigten Steuerungsoptionen bekommt man immer dann angeboten, wenn die zu einem Dienst gehörenden Profildaten geändert wurden.

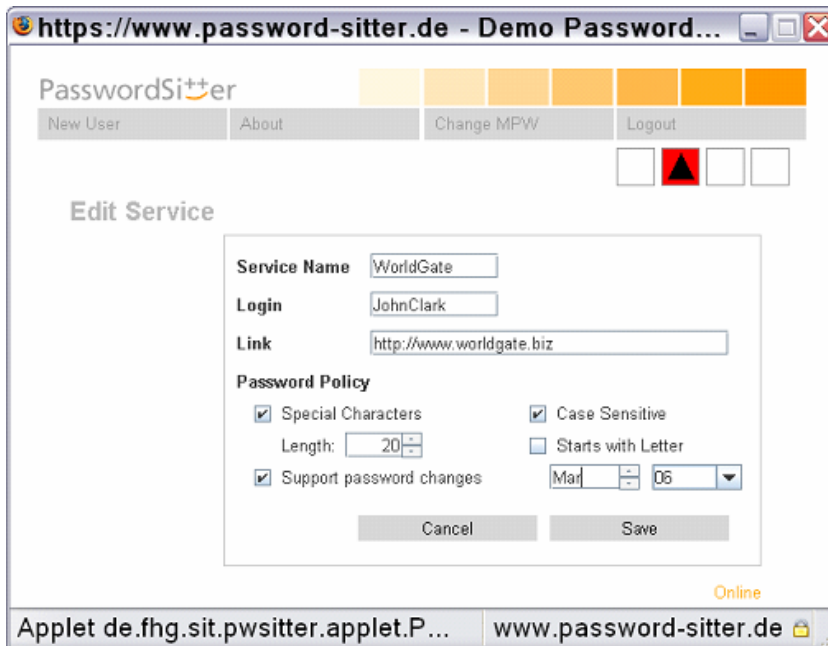


Abbildung 16: Die geänderten Profildaten von WorldGate



Abbildung 17: Unterstützung beim Passwortwechsel

Durch Anklicken der Option „Old Password“, berechnet der PasswordSitter das alte Passwort und legt dieses in der Zwischenablage zum einfachen Einfügen in das Formular zur



Passwortänderung ab. Wählt man danach die Option „New Password“, berechnet der PasswordSitter das neue Passwort und stellt dieses ebenfalls über die Zwischenablage bereit. Abbildung 18 zeigt die in einen Editor kopierten Passwörter für den Dienst „WorldGate“ vor und nach der Veränderung der Versionsangabe gemäß Abbildung 15 und Abbildung 16. Man kehrt man zur Profilübersicht zurück, indem man in Abbildung 17 die Option „Done“ auswählt.

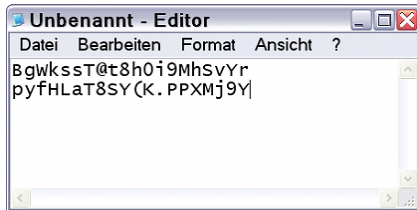


Abbildung 18: Altes und neues Passwort für WorldGate

Im Vorangegangenen wurde der PasswordSitter ausschließlich im Online-Modus betrieben, d.h. die Profildaten wurden von einer Datenbank geladen. Sollte die Datenbank nicht zur Verfügung stehen, dann hat man die Möglichkeit, den PasswordSitter im Offline-Modus zu betreiben. Hierzu wählt man beim Anmeldefenster des PasswordSitters die Option „Work Offline“ aus, wie in Abbildung 19 dargestellt. Im Gegensatz zum Online-Modus ist der Benutzernamen hier nicht erforderlich. Als Computernutzer gibt man im Offline-Modus lediglich das Master-Passwort ein. An dieser Stelle werden nun auch die Vorteile der Verwendung der optischen Rückmeldung —das schwarze Dreieck auf rotem Hintergrund— offensichtlich, welches dem Benutzer nach Eingabe des Master-Passworts angezeigt wird. Da im Offline-Modus keine Anmeldung bei der Datenbank erfolgt, würde man ohne derartige Rückmeldung zunächst nicht merken, wenn sich ein Tippfehler bei der Eingabe des Master-Passworts eingeschlichen hat. Ein falsch eingegebenes Master-Passwort hätte dann zur Konsequenz, dass die Passwörter falsch berechnet würden. Tippfehler können jedoch an der veränderten optischen Rückmeldung schnell erkannt werden.



Abbildung 19: Start des Offline-Modus beim PasswordSitter



Nach Eingabe des Master-Passworts und Betätigung des Login-Knopfes kann man auswählen, ob die Profildaten von der lokalen Festplatte geladen oder per Hand eingegeben werden sollen. Das Einlesen von der Festplatte führt mit einer angezeigten Liste von registrierten Diensten zum gleichen Ergebnis wie das Einlesen der Profildaten aus der Datenbank. Deshalb betrachten wir hier lediglich die Variante des Offline-Modus, bei welcher man die Profildaten von Hand eingibt.

Bei Auswahl dieser Variante des Offline-Modus öffnet sich für den Benutzer ein Fenster, in welches er die von ihm verwendete Dienstbezeichnung für den jeweiligen Dienst, seinen Login-Namen, die Passwortregeln und gegebenenfalls die optionale Versionsangabe eingibt. Sofern sich der Benutzer an diese Daten erinnern kann, gibt er diese ein und kann danach das Passwort für den Dienst berechnen. In Abbildung 20 wird das Passwort für den (Dummy-)Dienst „Secure Service“ berechnet, welches im Online-Modus bereits auch in Abbildung 10 berechnet wurde.

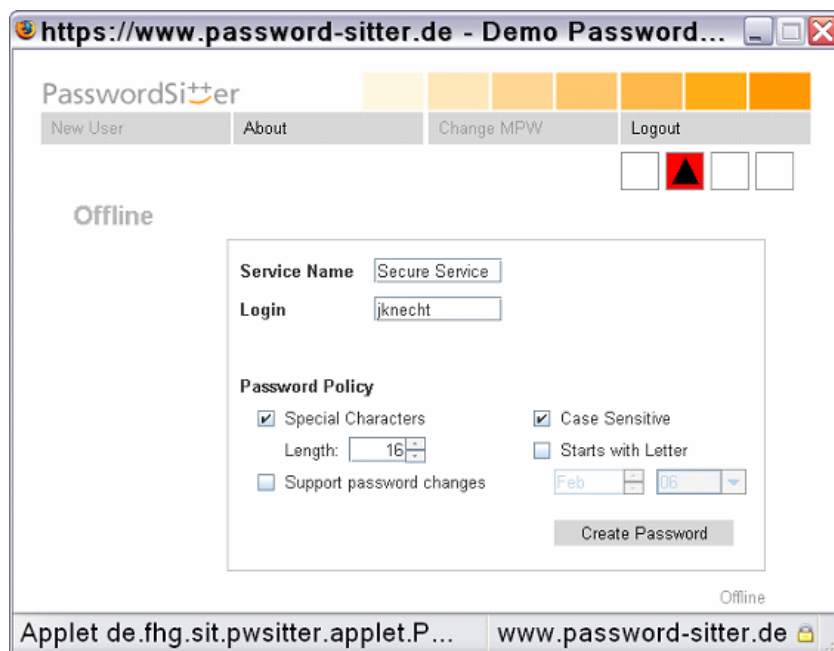


Abbildung 20: Verwendung des PasswordSitters im Offline-Modus

Auch wenn in dieser Variante des Offline-Dienstes Profildaten von Hand eingegeben werden müssen, so ist der Umfang der einzugebenden Daten sehr gering. Da die Profildaten bei der Verwendung des PasswordSitters im Online-Modus stets angezeigt werden, wird kontinuierlich dazu beigetragen, dass dem Benutzer die Erinnerung an diese Daten nicht zu schwer fällt. Die hier gezeigte Variante des Offline-Modus wird in Praxis wahrscheinlich eher selten verwendet werden. Als Computernutzer wird man es vorziehen, den Online-Modus oder die Variante des Offline-Modus mit lokaler Profilabspeicherung zu verwenden. Dennoch ist die Bereitstellung dieser Variante des Offline-Modus sinnvoll, da sie die Freiheit und Möglichkeiten von Nutzern stärkt. Durch diese ist es einem Nutzer möglich, auch an fremden Endgeräten und bei möglicherweise temporär ausgefallener Datenbank seine Passwörter zu generieren.

Eigenschaften des PasswordSitters

Der PasswordSitter bringt den Anwendern eine Reihe von Vorteilen im täglichen Umgang mit ihren Passwörtern. Diese lassen sich folgendermaßen zusammenfassen:



- 😊 Benutzerfreundlichkeit: Benutzer müssen sich nur noch ein Passwort merken —das Master-Passwort.
- 😊 Flexibilität und Freiheit: Die Passwörter stehen überall auf der Welt zur Verfügung, ohne dass der Benutzer Notizen oder Speicher-Token mit sich führen muss bzw. sich um die ständige Verfügbarkeit dieser Hilfsmittel kümmern muss.
- 😊 Verfügbarkeit: So lange sich der Benutzer an sein Master-Passwort erinnert, können die Passwörter nicht verloren gehen —da sie nirgendwo hinterlegt oder gespeichert sind.
- 😊 Plattformunabhängigkeit: Dank der eingesetzten Java-Technologie kann der PasswordSitter auf verschiedenen Plattformen eingesetzt werden.
- 😊 Endgeräteunabhängigkeit: Die Passwörter sind auf jedem Endgerät verfügbar. Selbst wenn ein Benutzer ein neues Passwort auswählt oder verändert, dann kann er ohne weiteres Zutun von jedem anderen Endgerät aus direkt auf das neue Passwort zugreifen.
- 😊 Kosten: Die Kosten für den PasswordSitter liegen deutlich unter den Kosten, die durch die heutige Passwort-Praxis entstehen. Der PasswordSitter kann in Unternehmen aktiv dazu beitragen, Kosten einzusparen.
- 😊 Konformität: Der PasswordSitter unterstützt die Generierung von Passwörtern, welche verschiedenen Passwort-Regeln genügen.
- 😊 Sicherheit: Der PasswordSitter verbessert die Sicherheit im heutigen Passwort-Management. Da eine Vielzahl von Systemen, Diensten und Anwendungen Passwortmechanismen einsetzen, ist es für deren Sicherheit unabdingbar, dass Passwortverfahren in der Praxis sicher betrieben werden können.

Da die Sicherheit in diesem Zusammenhang den zentralen Aspekt darstellt, sollen die Sicherheitseigenschaften des PasswordSitters an dieser Stelle nochmals detailliert aufgelistet werden. Der PasswordSitter bietet die folgenden Sicherheitseigenschaften:

- 😊 Aus der Kenntnis eines Passworts kann man nicht auf das Master-Passwort zurück schließen.
- 😊 Aus der Kenntnis eines Passworts kann man nicht auf ein anderes Passworts zurück schließen.
- 😊 Die vom PasswordSitter erzeugten Passwörter erfüllen die Sicherheitsanforderungen an gute Passwörter. Diese verfügen über eine entsprechende Länge und über zufällig ausgewählte Vertreter aus den geforderten Zeichenklassen. Die somit generierbaren Zeichenkombinationen sind in keinem Lexikon zu finden. Ein Beispiel für ein solches Passwort mit 20 Stellen, Klein- und Großbuchstaben, Ziffern und Sonderzeichen könnte lauten „3Gh%mk3!Bz7rjKDaZ+8w“.
- 😊 Die von dem Verfahren generierbaren Passwörter, welche die vorgegebenen Passwortregeln erfüllen, sind gleichverteilt. Das bedeutet, dass alle Zeichen aus den jeweiligen Zeichenmengen mit der gleichen Wahrscheinlichkeit auftreten.



- ++ Da der PasswordSitter als signiertes Applet angeboten werden kann, wobei das signierte Applet im Bedarfsfall über das Internet geladen wird, ist die Integrität des Codes gewährleistet. Dadurch kann ein Computernutzer sogar in einer fremden Umgebung an einem fremden Endgerät seine Passwörter erzeugen; und dies mit der Gewissheit, dass er sein Master-Passwort nicht an ein manipuliertes Programm übergibt.
- ++ Die Weitergabe von Passwörtern in Unternehmen kann unterbunden werden, da Benutzer ihre eigenen Passwörter gar nicht mehr kennen. Es ist zudem anzunehmen, dass Benutzer davor zurückschrecken, ihre Master-Passwörter weiter zu geben, da sie mit diesen anderen Zugang zu allen ihren Passwörtern geben würden.
- ++ Im Online-Modus ist der Zugang zu dem Server durch ein Passwort geschützt, so dass die von einem Computernutzer gespeicherten Profildaten weder von Unberechtigten eingesehen noch verändert werden können.
- ++ Die für den Offline-Modus auf ein Endgerät exportierten Profildaten werden auf diesem Endgerät verschlüsselt abgespeichert.
- ++ Aus dem Server-Passwort ist es nicht möglich, auf das Master-Passwort zurück zu schließen.
- ++ Die über den Server erreichbare Datenbank mit den Benutzerprofilen ist gegen SQL-Injection-Angriffe gesichert.
- ++ Online-Angriffe werden abgewehrt indem IP-Adressen, von denen eine bestimmte Anzahl von Fehlversuchen zur Datenbankanmeldung ausgehen, für eine gewisse Zeit blockiert werden.

Für wen sollte der PasswordSitter interessant sein?

Die Verwertung des PasswordSitters kann für unterschiedliche Unternehmen interessant sein. Unternehmen, die vom PasswordSitter profitieren können, lassen sich beispielsweise in die folgenden Kategorien einordnen:

- ++ PasswordSitter für Unternehmen als Endanwender: Unternehmen, die eine Reihe von Diensten und Anwendungen betreiben, bei welchen sich ihre Mitarbeiter mittels Passwörtern anmelden, können mit dem PasswordSitter Zeit und Kosten sparen, die bisher durch Probleme beim Passwortmanagement und durch Sicherheitsschwachstellen im Zusammenhang mit Passwörtern entstanden sind. Solche Unternehmen können die PasswordSitter-Lösung — Server und Clients — gewinnbringend in ihre IT-Infrastruktur integrieren. Bei besonderen Anforderungen kann der PasswordSitter individuell für die Belange des Endanwenders angepasst werden.
- ++ PasswordSitter für IT-Dienstleister: IT-Dienstleister, welche die IT-Infrastruktur anderer Unternehmen aufbauen und betreiben, können ihr Produkt- und Dienstportfolio durch das Angebot des PasswordSitters ergänzen, damit ihre Kunden als Endanwender durch verbessertes Passwortmanagement Kosten sparen können. Dies ermöglicht ihren Kunden die Konzentration auf das Kerngeschäft, ohne dass der alltägliche Einsatz von Informations- und Kommunikationstechnologie zusätzliche Ressourcen verschlingt.



- ++ PasswordSitter für Software-Hersteller: Für Software-Hersteller besteht die Möglichkeit, den PasswordSitter in ihre Produkte zu integrieren, um die eigenen Produkte gegenüber dem Angebot von Konkurrenten positiv abzugrenzen. Die Ausübung von Schutzrechten erlaubt die Erteilung von branchenspezifischen Exklusivnutzungsrechten.
- ++ PasswordSitter für Portalbetreiber: Portalbetreiber können die Funktionalität des PasswordSitters in ihr Portal integrieren und darüber ihren Endkunden einen Dienst für das sichere und benutzerfreundliche Passwortmanagement anbieten. Die Bereitstellung eines zentralen Dienstes für das Passwortmanagement in einem Portal steigert dessen Attraktivität und kann somit zur Kundenbindung beitragen, da Kunden das Portal regelmäßig besuchen müssen.

Schlussbemerkung

Der PasswordSitter bietet eine sichere und benutzerfreundliche Lösung zum Passwort-Management. Da die überwiegende Zahl von Diensten und Anwendungen zur Authentifizierung von Benutzern Passwortverfahren einsetzen, ist es erforderlich, dass gewisse Anforderungen an das Passwort-Management erfüllt sind. Bei der stark gestiegenen Anzahl von registrierten Diensten und Passwörtern, die sich ein Benutzer merken muss, sind die Anforderungen von Sicherheitsexperten an starke Passwörter, die für den Computernutzer dennoch stets verfügbar sind, heute ohne weitere technische Hilfsmittel nicht mehr zu erfüllen.

Der PasswordSitter bietet ein solches technisches Hilfsmittel. Er unterstützt die Benutzer beim Passwort-Management und spart Unternehmen Kosten und Anwendern Zeit und viel Ärger. Mit nur noch einem zu merkenden Geheimnis hat man alle seine starken Passwörter zu jeder Zeit, an jedem Ort, für jeden Dienst und auf jedem Endgerät verfügbar, ohne dass man die Passwörter als Benutzer hierzu mit sich führen muss bzw. diese über Internet zugreifbar hinterlegt.

Kontakt

Dipl.-Inform. Ruben Wolf
Fraunhofer Institut für Sichere
Informationstechnologie SIT
Rheinstraße 75
64295 Darmstadt
Telefon: 06151 – 869 – 60177
Telefax: 06151 – 869 – 224
E-mail: ruben.wolf@sit.fraunhofer.de

Dr.-Ing. Markus Schneider
Fraunhofer Institut für Sichere
Informationstechnologie SIT
Rheinstraße 75
64295 Darmstadt
Telefon: 06151 – 869 – 4707
Telefax: 06151 – 869 – 224
E-mail: markus.schneider@sit.fraunhofer.de

