iMobileSitter: Sicheres Passwortmanagement in Zeiten von digitalen Schlüsseldiensten und Advanced Persistent Threats

Der iMobileSitter akzeptiert jede Eingabe und entschlüsselt bei jedem Master-Passwort den Passwort-Container. Ob es sich jedoch um die echten gespeicherten Passwörter handelt, weiß nur der berechtigte Benutzer.

Immer mehr Benutzer vertrauen ihre Zugangsdaten wie Passwörter und PINs einer Software zur Passwortverwaltung an. Der Schutzumfang, den eine konventionelle Passwortverwaltung bietet, genügt heute in Zeiten digitaler Schlüsseldienste und entsprechender Werkzeuge nicht mehr. Das Fraunhofer SIT hat mit dem iMobileSitter einen Passwortspeicher entwickelt, der Angriffen mittels dieser Schlüsseldienste und Werkzeuge standhält.

Von Ruben Wolf, Frederik Franke und Markus Schneider, Fraunhofer SIT/CASED

Ein typischer Benutzer braucht heute so viele Zugangsgeheimnisse, zum Beispiel Passwörter oder PINs, dass er sich diese kaum noch merken kann. Wenn man sich an alle Sicherheitshinweise hält, wie etwa sich die eigenen Passwörter so auszuwählen, dass sie nicht einfach von anderen geraten werden können, und auch nie das gleiche Kennwort für verschiedene Zugänge zu verwenden, dann stößt man als Mensch schnell an seine Erinnerungsgrenzen. Das gilt insbesondere dann, wenn bestimmte Passwörter nicht sehr häufig benötigt werden. Für solche Benutzer sind Werkzeuge zur Verwaltung von Zugangsgeheimnissen praktisch unersetzlich.

Sicherheit von Managementwerkzeugen

Vom Prinzip her ähneln diese Werkzeuge dem klassischen Schlüsselbund. Kommt dieser einmal abhanden, dann hilft der Schlüsseldienst. Wenn man Sorge hat, dass der Schlüsselbund in fremden Händen sein könnte, wechselt man zusätzlich die Schlösser aus. Bei den in einem digitalen Schlüsselbund gespeicherten Daten ist hingegen nicht mehr klar, wann Schlösser sinnbildlich auszuwechseln sind, da nicht notwendigerweise bemerkt wird, wenn die Daten in fremde Hände gelangen, da sich ein Fremder einfach eine Kopie der Datei mit den gespeicherten Zugangsdaten verschaffen kann. Ein solcher Kopiervorgang ist denkbar, ohne dass der eigentliche Besitzer der Datei davon etwas mitbekommt. Zum Schutz gegen solche Angriffe werden die Zugangsheimnisse verschlüsselt, in der Hoffnung, dass Angreifer keinen Zugriff auf die Zugangsdaten haben. Bei konventionellen Produkten werden die Daten so verschlüsselt, dass zur Ver- und Entschlüsselung der kryptographische Schlüssel aus einem Master-Passwort abgeleitet wird. Doch diese Art der passwortbasierten Verschlüsselung birgt in der Praxis eklatante Sicherheitsrisiken, wie gerade von Elcomsoft bestätigt wurde [Elc12, BS12]. Die mit konventionellen Passwortspeichern verschlüsselt gespeicherten Zugangsdaten lassen sich nämlich auch dann in Erfahrung bringen, wenn Passwortspeicher sichere kryptographische Verfahren einsetzen, zum Beispiel AES. Die Daten können entschlüsselt werden, ohne dass kryptographische Verfahren gebrochen werden müssen. Hierzu gibt es mittlerweile ein gutes Angebot von entsprechenden Werkzeugen. Wer sich nicht selbst Werkzeuge beschaffen möchte, der kann digitale Schlüsseldienste beauftragen. Auch hierzu gibt es mittlerweile ein breites Angebot von Dienstleistungen, insbesondere als Cloud-Angebote [Gar11, heise-ix09, heise10, heise11]. Hinzu kommt, dass Cloud-basierte Schlüsseldienste im Vergleich zu konventionellen Schlüsseldiensten sehr viel günstiger sind. Werkzeuge und Dienstangebote nutzen Wörterbuchangriffe oder sogar Brute-Force-Angriffe, um den Schlüssel zur Entschlüsselung in Erfahrung zu bringen. Liegen Hackern die verschlüsselten Daten konventioneller Speicher vor, dann kommen sie an die hinterlegten Zugangsgeheimnisse ran und können sich bei den entsprechenden Zugängen bedienen. Von diesen Angriffen bekommt man als Geschädigter in der Regel leider erst dann etwas mit, wenn es zu spät ist.

Durch Schütteln des iPhones werden Zufallszahlen für die Verschlüsselung erzeugt.

Die Risiken unsicherer Verwaltung

Die Sicherheit der Zugangskontrolle kann beeinträchtigt werden, auch wenn Benutzer die Hinweise für sichere Auswahl und Umgang mit Zugangsgeheimnissen umsetzen. Die Unsicherheit der Verwaltungssoftware für Geheimnisse wirkt hierbei negativ auf die Sicherheit der eigentlich zu schützenden Zugänge zurück. Nach geglücktem Wörterbuchangriff können mögliche Vorkehrungen wie etwa die Sperrung von Zugängen nach einer bestimmten Anzahl von Fehlversuchen bei der Passworteingabe keine Wirkung mehr entfalten. Die dadurch entstehenden Risiken können sehr hoch sein. Dies gilt insbesondere dann, wenn Angreifer es auf bestimmte Personen abgesehen haben, welche ganz gezielt mit hohem Aufwand und professionell organisiert angegriffen werden. So etwas geschieht meistens, um über diese Personen an wertvolle Informationen zu gelangen, zum Beispiel für Wirtschaftsspionage. Diese Bedrohung wird unter dem Begriff Advanced Persistent Threats als abstraktem Modus Operandi diskutiert [Pot10]. Gerade hochrangige Entscheider mit Zugang zu sensiblen Daten stehen im Fokus solcher Angriffe [Mül11]. Die jährlichen Schäden für die deutsche Wirtschaft gehen weit in die Milliarden Euro [SpiegelOnline12]. Hacker testen bei solchen Angriffen viele verschlungene und komplizierte Wege durch IT-Systeme aus. Umso einfacher wird es, wenn sie ohne besonderen Aufwand an Passwörter von Entscheidern gelangen können. Ein Beispiel für Industriespionage durch kompromittierte Zugangsgeheimnisse hat der mittlerweile zerschlagene Telekom-Ausrüster Nortel geliefert. Es ist also eminent wichtig, dass die Zugangsdaten angemessen gesichert werden.

Unsicherheit trotz sicherer Kryptoverfahren bei konventionellen Produkten

Doch wo liegt das eigentliche Problem bei den konventionellen Produkten zur Verwaltung von Zugangsdaten? Der Kern des Problems besteht darin, dass erstens diese Produkte auf passwortbasierte Verschlüsselung setzen und zweitens man bei Entschlüsselungsversuchen erkennen kann, ob ein getestetes Master-Passwort korrekt ist oder nicht. Die konventionellen Produkte erfüllen nicht die Voraussetzungen zur sicheren Anwendung der als sicher angenommenen Verfahren. Starke Verschlüsselungsverfahren wie AES haben heute Schlüssellängen von mindestens 128bit. Die darüber entstehende Schlüsselmenge hat größenordnungsmäßig 10^{38} Elemente. Eine wesentliche Sicherheitsforderung von Verschlüsselungsverfahren besteht darin, dass ein Schlüssel möglichst zufällig aus der vollständigen Schlüsselmenge ausgewählt wird. Die in den konventionellen Produkten über die Master-Passwörter adressierte Menge der Schlüssel macht jedoch in der Regel nur eine winzig kleine Teilmenge der gesamten Schlüsselmenge aus. Verbunden mit der Rückmeldung bei Entschlüsselungsversuchen werden dadurch Wörterbuchangriffe oder Brute-Force-Angriffe möglich. Sie können durchgeführt werden, ohne dass sie von den Angegriffenen bemerkt werden.

Lösungsansätze

Das Problem ließe sich etwa dadurch entschärfen, indem man die Benutzer dazu bringen würde, vergleichsweise lange und sichere Master-Passwörter auszuwählen. Dadurch würden Produkte zur Passwortverwaltung jedoch benutzerunfreundlich werden. Ein anderer denkbarer Ansatz könnte darin bestehen, dass man die Ableitung der kryptographischen Schlüssel aus dem Master-Passwort durch künstlichen Aufwand verzögert. Dies wird in der Praxis tatsächlich gemacht, zum Beispiel über geeignete Parametereinstellung der Schlüsselableitungsfunktion PBKDF2 bei PKCS#5. In der Realität hat das jedoch seine Grenzen. Tests des Fraunhofer SIT haben ergeben, dass sich allein bei mobilen Endgeräten die Berechnungszeiten aufgrund unterschiedlicher Rechenleistung um einen Faktor 10^7 unterscheiden, was in der Praxis dramatische Konsequenzen hätte. Wäre die PBKDF2-Rundenanzahl so eingestellt, dass die Ableitung eines Schlüssels auf einem schnellen Gerät 1 Sekunde brauchen würde, dann würde jede Entschlüsselung eines Geheimnisses auf einem langsamen Gerät 10^7 Sekunden (ca. 116 Tage) benötigen. Geht man also davon aus, dass verschlüsselte Daten zwischen verschiedenen Plattformen synchronisiert werden sollen, dann muss die Schlüsselableitung so eingestellt sein, dass auch langsame Geräte die Entschlüsselung in vertretbarer Zeit ausführen können. Das hat jedoch den Nachteil, dass auch Wörterbuchangriffe schneller ausgeführt werden können.

Die Lösung von Fraunhofer SIT

Am Fraunhofer SIT hatte man zur Lösung des Problems eine andere

Idee: Es wurde ein Verfahren entwickelt, bei dem ein Hacker oder eine Hacker-Software bei der Eingabe eines Master-Passworts nicht erkennen kann, ob er – oder sie – fündig wurde. Nach Eingabe eines Master-Passworts werden immer Daten entschlüsselt, die so aussehen, als könnten sie korrekt sein. Bei jedem Versuch muss das entschlüsselte Zugangsgeheimnis bei dem jeweiligen Zugang eingegeben werden. So wird der Hacker in seinem Tun ausgebremst und kann praktisch keine Wörterbuchangriffe durchführen.

Im Kern dieses Verfahrens steckt eine AES-basierte CBC-MAC-Berechnung als Pseudozufallsgenerator. Ausgehend von einem rein zufällig gewählten Startzustand des Pseudozufallsgenerators wird dieser zur Verschlüsselung eines Zeichens so lange getaktet, bis seine Ausgabe mit dem zu verschlüsselnden Zeichen übereinstimmt. Die Codierung ist hierbei so gewählt, dass alle Ausgaben auf je ein erlaubtes Klartextzeichen abgebildet werden können. Als Chiffrat wird der Zustand gespeichert, bei dem die Ausgabe mit dem zu verschlüsselnden Zeichen übereinstimmt. Zur Entschlüsselung wird der Zustand als Chiffrat und der Schlüssel eingegeben, so dass die entsprechende Ausgabe des Pseudozufallsgenerators reproduziert werden kann, die im nächsten Schritt mittels Codierungstabelle auf das Klartextzeichen abgebildet wird.

iMobileSitter – Sichere Passwortverwaltung für das iPhone

Auf Basis dieses Verfahrens wurde nun für das iPhone ein Passwortmanager entwickelt. Die Software heißt iMobileSitter und ist für Benutzer nicht schwieriger zu bedienen als konventionelle Passwortspeicher. Für Angreifer wird es jedoch viel schwieriger. Die Software akzeptiert jede Eingabe und entschlüsselt bei jedem Master-Passwort die vermeintlichen Geheimnisse. Ob es jedoch die richtigen sind, weiß nur der berechtigte Benutzer. Denn jedes berechnete Ergebnis sieht so aus, als ob es richtig sein könnte. Wird beispielsweise eine vierstellige PIN entschlüsselt, so wird stets eine entsprechende Zahlenkombination berechnet. Hacker oder Hacker-Software können nicht erkennen, ob der Versuch erfolgreich war. Jedes berechnete Ergebnis muss bei dem Zugang ausprobiert werden. Dort können dann die Sicherungsmechanismen bei Fehleingabe greifen, zum Beispiel Sperrung der EC-Karte nach drei falschen Eingaben am Geldautomaten.

Die Software verschlüsselt nur das Passwort, nicht aber Verwendungszweck und Benutzernamen. Dahinter steckt ein wichtiger Aspekt beim Schutz gegen Wörterbuchangriffe: Login-Namen wie beispielsweise die E-Mail-Adresse sind oft bekannt. Wenn diese Informationen also verschlüsselt und einem Hacker bekannt wären, dann könnte er so lange Master-Passwörter testen, bis die ihm bekannte Information angezeigt wird.

Mit einem falschen Master-Passwort kommt man zwar nicht an die Geheimnisse, jedoch lassen sich damit die gespeicherten Daten löschen oder verändern. Was zunächst wie eine Schwachstelle erscheinen mag, ist beabsichtigt und für die Geheimhaltung der Daten unbedingt erforderlich. Der Angreifer soll in keinem Fall eine Rückmeldung bekommen, ob das eingegebene Master-Passwort richtig ist. Würde man die Daten nur verändern können, wenn das richtige Master-Passwort eingegeben wurde, dann könnte man dies wieder für Wörterbuchangriffe nutzen. Der Abwägung zwischen den verschiedenen Schutzzielen liegt die Annahme zugrunde, dass bei geheimen Zugangsdaten die Geheimhaltung sehr viel wichtiger ist als deren Schutz gegen Veränderung. Bei Verlust oder Diebstahl des Smartphones ist es dem Eigentümer wahrscheinlich weniger wichtig, ob ein Hacker Daten verändern kann. Darüber hinaus ist anzunehmen, dass der Hacker wahrscheinlich wenig eigenen Nutzen aus einer Datenmodifikation ziehen kann. Zudem ist klar, dass ein Zugriffsschutz auf der Ebene des Passwortmanagers wenig hilft, da Hacker ohnehin immer im Dateisystem die Datei mit den verschlüsselten Daten löschen können. Dieser Weg ist auch bei konventionellen Produkten möglich. Insofern ist der Zugriffsschutz gegen Veränderung bei konventionellen Passwortmanagern ohnehin kein echter Schutz. Das beste Mittel gegen Angriffe durch Löschen oder Veränderung ist das regelmäßige Anlegen von Backups, die im Bedarfsfall wieder eingespielt werden können. Diese Backups müssen natürlich verschlüsselt sein. iMobileSitter verschlüsselt die Daten immer in gleicher Weise, ganz gleich ob sie auf dem iPhone gespeichert sind oder auf einen anderen Speicher exportiert werden.

Für die Verschlüsselung braucht die Software echte Zufallszahlen. Und um die zu erzeugen, muss man sein iPhone einfach nur kräftig schütteln.

Entwickelt wurde iMobileSitter von Fraunhofer SIT, vertrieben wird die Software über den iTunes-Store von Apple. Weitere Informationen gibt es unter www.imobilesitter.com. Die Android-Version dieser Software ist in Entwicklung; sie soll in der zweiten Jahreshälfte 2012 auf den Markt kommen.

Referenzen

[BS12] A. Belenko, D. Sklyarov: "Secure Password Managers" and "Military-Grade Encryption" on Smartphones: Oh, Really? http://www.elcomsoft.com/WP/BH-EU-2012-WP.pdf, 2012

[Elc12] Elcomsoft: ElcomSoft Analyzes 17 Smartphones' Secure Password Managers, Finds No Security. http://www.elcomsoft.com/PR/PK_120316_en.pdf, 2012

[Gar11] S. Garfinkel: Angriff aus der Wolke. Technology Review, Oktober 2011

[heise-ix09] heise / iX: Preiswert Schlüssel knacken in der Cloud. November 2009, http://www.heise.de/ix/meldung/Preiswert-Schluessel-knacken-in-der-Cloud-848574.html

[heise10] heise: GPUs knacken Passwörter in der Cloud. November 2010, http://www.heise.de/security/meldung/GPUs-knacken-Passwoerter-in-der-Cloud-1138949.html

[heise11] heise: WPA-Schlüssel in der Cloud knacken. Januar 2011 http://www.heise.de/security/meldung/WPA-Schluessel-in-der-Cloud-knacken-1168061.html

[Mül11] E. Müller: Voller Durchblick. Manager Magazin, November 2011, http://www.manager-magazin.de/lifestyle/artikel/0,2828,794488,00.html

[Pot10] B. Potter: Thinking Operationally. IEEE Security & Privacy, May/June 2010

[SpiegelOnline12] Spiegel Online: Studie zur Industriespionage - Jeder zweite deutsche Konzern wird ausgespäht. April 2012, http://www.spiegel.de/wirtschaft/unternehmen/0,1518,829055,00.html