Inhalt

2. Inselbegabung wäre nützlich
1. Spinnen hangeln sich durch das Netz
    1. Sei so „schlau“ wie der Anwender
    2. Heute ist der Müller dran!
    3. Und wieder Salz in der Suppe?
    4. Was hilft?
        1. Ein gutes Passwort
        2. Was muss der Passwort Manager bieten?
    5. Welche Eigenschaften muss ein guter Passwort Manager haben?

Sofern Sie die vorangegangenen Artikel [„Weißt Du wieviel Sternlein stehen„, „Schlüssel,Salz und Regenbogen„] gelesen haben, gehören Sie inzwischen ja schon eher zu den Wissenden im Bereich der Verschlüsselung.

Was Sie auf jeden Fall mitgenommen haben sollten ist, dass ein s.g. **Brute-Force Angriff**, bei dem man also alle möglichen Passwörter/Schlüssel der Reihe nach durchtestet, derart unglaublichen Aufwand verursacht, dass er für die Praxis kaum relevant ist.

*

Inselbegabung wäre nützlich *

Angenommen, Sie melden sich bei einer WEB-Seite an. Dann werden Sie dort meist nach einem Benutzernamen und einem Passwort gefragt.

Auch wenn ich seit Jahren nicht müde werde, auf bestimmte Gefahren hinzuweisen, weiß ich doch, dass oft die Bequemlichkeit siegt und folgende Kardinalfehler begangen werden.

1. Es wird ein sehr **einprägsames** Passwort verwendet. Je seltener man eine Seite besucht, desto einprägsamer muss es sein.

2. Da das massenhafte Einprägen sicherer Passwörter eine Inselbegabung voraussetzt, verwendet man **dasselbe Passwort** natürlich zu jeder sich bietenden Gelegenheit.

Daraus entstehen die folgenden Gefahren:

1. Einprägsame Passwörter sind meist **miserable Passwörter**. Sie bestehen aus Wörtern oder Begriffen, die genau so im Internet (*in s.g. Wörterbüchern*) zu finden sind oder haben einen direkten Bezug zur Person.
2. Wird eine der WEB-Seiten „gehackt" sind alle Seiten in Gefahr, auf denen Sie dasselbe Passwort benutzt haben.

Der zweite Punkt leuchtet sicher ein. Falls nicht, hilft folgende Erklärung: Mit den Zugangsdaten, die Angreifer auf der gehackten WEB-Seite erbeutet haben, gehen sie auf die **Großen im Internet** los. Mit Hilfe spezieller Programme wird versucht, sich mit den Daten in Seiten wie Amazon, eBay, Facebook, PayPal usw. einzuloggen. Natürlich fehlt auch kein Besuch bei den Online-Banken.

Die Gefahr, die aus der **Verwendung von Begriffen und Wörtern** erwächst offenbart sich, wenn man um die Werkzeuge der Angreifer weiß.

Wer unsere ArchiCrypt Programme kennt, der kennt die Analysefunktion bei der Eingabe eines neuen Passwortes. Dort kann man dann bisweilen lesen, dass sich die eingegebene Zeichenfolge vermutlich direkt im „**Hackerwörterbuch**" befindet. Was ist das für ein Wörterbuch? Was steht im Wörterbuch und wie wurde es erzeugt?

Spinnen hangeln sich durch das Netz *

Vielleicht haben Sie schon einmal den Begriff **WEB-Spider** (*Netz Spinne*) gehört. Es handelt sich dabei um Programme, die sich wie eine Spinne durch das Netz (Internet) hangeln. Man gibt eine Startseite vor. Diese Startseite wird dann vom WEB-Spider besucht und untersucht. Findet er einen Link (Verweis auf eine andere Seite), folgt er diesem und führt auch auf dieser Seite seine Analysefunktionen durch. Auch auf der neu besuchten Seite wird jedem Link gefolgt. Das Programm wandert also komplett selbstständig durch das Internet. Wir haben unserer „Spinne" beigebracht, die Seite in

die dort verwendeten Begriffe zu spalten und diese zu speichern. Jedes Vorkommen eines Begriffes wird natürlich nur einmal gespeichert. Herausgekommen ist eine **Datenbank, die 26 Millionen Wörter, Begriffe und Zeichenfolgen** enthält. Mit in diese Liste sind auch kursierende **Passwortlisten** eingeflossen.

> Googeln Sie doch einmal nach „Passwort Liste“ oder „password list“! Sie werden überrascht sein. Wenn Sie ein wenig recherchieren, sind Sie sicher auch überrascht, wie die Dateien entstanden (Hinweis: Meist durch Diebstahl von Zugangsdaten).

Sei so „schlau“ wie der Anwender *

Mit dieser Liste könnten Sie bereits massenhaft Zugänge zu Internetseiten knacken! Will eine etwas höhere Erfolgsquote bei einem Angriff erzielen, wendet man auf die Zeichenketten im Wörterbuch noch einige **Regeln** an, mit denen man Varianten der Wörter erzeugt.

1. Regel: Mache bewußt Schreibfehler
So wird aus Elefant ein Elevand
2. Regel: Ersetze Buchstaben durch Zahlen
Aus Elefant wird ein 3lefan1

3. Regel: Ersetze Buchstaben durch Sonderzeichen
Aus Charlie wie so (harlie
Aus Wasser wird Wa$$er

4. Regel: Verwende ein paar Ziffern (Geburtstage)
Aus Elefant wird 77Elefant1309

5. Regel: Spiegle die Wörter
Aus Elefant wird ein tnafelE

6. Regel: Wiederhole die Zeichen in einem Wort

Aus Elefant wird ElefantE, ElefantEl, … ElefenatElefant

Dadurch wird die Liste natürlich ordentlich aufgeplustert. Dennoch bewegt man sich in Größenordnungen, bei denen sich hinsichtlich des Aufwands keine Probleme ergeben. Man hat gegenüber einem **Brute-Force** Angriff einen verschwindend geringen Aufwand.

Wenn man die Muße besitzt, kann man sich auch gleich den Hashwert der Begriffe ausrechnen. Dadurch hat man dann ein prima Nachschlagewerk (*man sucht zu einem Hashwert den man erbeutet hat das zugehörige Passwort*), wenn man die Hashtabelle der Passwörter vom Server stiehlt. Wer nicht mehr weiß, was es mit Hashwerten auf sich hat, der kann das noch einmal in „Schlüssel,Salz und Regenbogen“ nachlesen.

Solch einen Angriffe nennt man Wörterbuchangriff (*Dictionary Attack*)

Dieses Verfahren ist unglaublich effektiv. Die Gründe haben wir ganz oben gesehen. Bequemlichkeit und fehlende Inselbegabung führen dazu, dass eben genau diese im Wörterbuch enthaltenen Begriffe von uns verwendet werden. Besonders erfolgreich ist man dann, wenn man dieses Verfahren gegen eine ganze Gruppe von Personen anwendet. Es sind immer einige darunter, die Passwörter nach allen Regeln der Kunst verwenden und damit jedem Angriff wiederstehen. Man kann aber sicher sein, dass ein nicht unerheblicher Anteil äußerst „bescheidene“ Passwörter nutzt. Mehr möchten Angreifer meist nicht.

Heute ist der Müller dran! *

Hat ein Angreifer es auf eine bestimmte Person abgesehen, kann er noch ein Spezialverfahren einsetzen. Im Falle eines Falles kommt er mit **personenbezogener Recherche** weiter.

Angenommen, der Angreifer hat es auf den Müller abgesehen. Dann wird eine Recherche in seinem sozialen Umfeld mit hoher Wahrscheinlichkeit zielführend sein.

Alle Namen und Vornamen in seinem Verwandten und Bekanntenkreis, Hunde, Katzen, Vögel, Hamster, tot oder lebendig, Hobbies, Bücher, Lieblingsessen, Automarken, Uhrenmarken, Parfums, Klammotten, Farben, Musik, Aufenthaltsorte, Hersteller des

Rechners, der Büromöbel, des Monitors, der Computermaus, Kontonummer, Bankleitzahl, Zahnarzt, Telefonnummern. Müll, vor allem Papiermüll, wird ausgewertet. Sie sehen worauf das hinausläuft und ahnen schon, dass es gar nicht so schwer ist, so eine Sammlung aufzubauen.

Aus den Rechercheergebnissen wird schließlich ein spezielles Wörterbuch aufgebaut, indem man alle möglichen Kombinationen der Begriffe testet. Sie würden sich aus zwei Gründen wundern!

1. Wie einfach es ist, sich eine solche Liste zu erstellen
2. Wie erfolgreich dieses System ist

> **Man muss nur das, was Müller hat, unbedingt haben wollen. Dann ist auch der Aufwand relativ.**

Im Zeitalter des in sozialen Netzwerken gelebten Exhibitionismus kann man sich das Wühlen im Müll oft auch sparen.

Und wieder Salz in der Suppe? *

Mit **Salz** (***Salt***) haben wir uns ebenfalls bereits beschäftigt. Damit haben wir den Anwendern von Rainbow-Tables den Wind aus den Segeln genommen.

> **Hilft Salz auch im Falle eines Wörterbuchangriffs?**
>
> **Nein, nicht wirklich!**
>
> [**Anmerkung:**
> *Im Weiteren hilft es, wenn wir den Begriff Schlüsselraum kennen. Ein Schlüsselraum ist die Menge aller theoretisch möglichen Schlüssel (Passwörter). Sie erinnern sich vielleicht. Bei AES (advanced encryption*

standard) in der 256 BIT Version gibt es die unglaubliche Anzahl von 2^{256} *Schlüsseln. Das sind* $1{,}16\times10^{77}$ *verschiedene Schlüssel.*]

Mit unserem Wörterbuch haben wir die im Vergleich zu einem **Brute-Force Angriff** notwendige Zahl zu prüfender Schlüssel drastisch reduziert.

Bei Brute-Force sehen wir uns ja dem gesamten Schlüsselraum gegenüber. Statt 10^{77} testen wir nur noch einen kleinen, aber von vielen Anwendern genutzten Teil des Schlüsselraums. Nämlich etwa 26 Millionen Passwörter respektive Schlüssel. Das sind nur 26×10^{6} Schlüssel. Mit den Varianten aus den Regeln von oben vielleicht 10^{9} Schlüssel.

Wenn Sie diese Zahlen einmal voneinander abziehen, dann werden Sie sehen, dass bei 10^{77}-10^{9} immer noch 10^{77} auf dem Display Ihres Taschenrechners erscheint.

Wir tasten also nur einen verschwindend geringen Teil des Schlüsselraums

ab und sind doch derart erfolgreich. Erstaunlich!

Da der zu beackernde Schlüsselraum so winzig ist, hilft hier auch das „Salz“ nicht wirklich. Nämlich dann nicht, wenn wir so dumm waren und einen Begriff aus dem Wörterbuch gewählt haben.

Sie wissen ja, Salt wird und muss nicht geheim gehalten werden. Folglich hat ein Angreifer diesen Wert wahrscheinlich zur Verfügung und kann sich die Hashwerte mit den Begriffen aus dem Wörterbuch zusammen mit dem Salt-Wert leicht neu berechnen. Dieser Aufwand ist immer noch überschaubar.

Was hilft? *

Sie wissen es selbst bereits. Inzwischen verfügen Sie über ausreichend Kenntnisse und verstehen die Forderungen.

Ein gutes Passwort *

1. Verwenden Sie keine Begriffe, sondern möglichst zufällige Zeichenfolgen, bestehend aus Ziffern, Groß-/Kleinbuchstaben und Sonderzeichen. Das Passwort sollte nach heutigem Stand eine Länge von 12 Zeichen haben.
2. Verwenden Sie ein Passwort immer nur für eine Sache. Also bei jeder WEB Seite ein neues Passwort generieren.

Man kann diese Daten nicht selbst in seinem Kopf oder auf einem Blatt Papier verwalten (*das dann möglichst noch auf dem Schreibtisch liegt*)! Sie brauchen ein **Hilfsmittel**. Einen guten Passwort Safe, der Ihnen die Verwaltung dieser Daten auch abnimmt. Klar, dass ich Ihnen an dieser Stelle ArchiCrypt Passwort Safe ans Herz lege. Es würde mich freuen, da wir uns darüber finanzieren.

Letztlich wichtig ist hingegen nur, dass Sie überhaupt ein solches Programm verwenden, um eben die Fallstricke zu umgehen. Natürlich geht das eventuell auch mit einem Konkurrenzprodukt.

Was muss der Passwort Manager bieten? *

Muss er gut aussehen? Sagen wir einmal so: Es schadet wirklich nicht, hilft aber auch nicht, wenn es mit der Sicherheit hapert!

Welche Eigenschaften muss ein guter Passwort Manager haben?

*

1. Das Programm sollte ein **anerkanntes modernes Verschlüsselungsverfahren** anwenden. Dazu zählen aus meiner Sicht die Verfahren **AES** (*advanced encryption standard*), **Blowfish**, **Twofish**).
2. Im Prinzip implizit in 1 enthalten. **Finger weg von** angeblich hochsicheren **selbstentwickelten Verfahren** mit Traumschlüssellängen und ausstehender Patentierung. Selbst wenn es ein Patent gäbe, prüft im Patentamt kein Mensch ob der Algorithmus sicher ist!
3. **Finger weg von alten**, nicht mehr gepflegten **Programmen**. Sie setzen unter Umständen Verfahren ein, die längst nicht mehr als sicher gelten (z.B. DES)
4. Das Programm darf Ihr Passwort zur Absicherung der Passwörter nicht direkt nutzen, sondern muss es zusammen mit einem zufälligen, bei jeder Neuerzeugung einer Datenbank oder Datei neu generierten **Salt-Wert** verknüpfen.
5. Salt-Wert und Nutzerpasswort müssen mittels einer s.g. **Schlüsselableitungsfunktion** (*key derivation function*) und einer ausreichend **hohen Rundenzahl** in den eigentlichen Schlüssel transformiert werden. [Für Interessierte: *ArchiCrypt Passwort Safe berechnet aus dem Salt-Wert und dem Nutzerpasswort mittels einer Ableitungsfunktion PBKDF vom Typ 2 und SHA512 als Hashfunktion den eigentlichen Schlüssel. Dabei werden 50.000 s.g. Runden angewendet.*]
   Was erreicht man hier? Sie haben weiter oben gesehen, dass es durchaus interessant sein kann, für einen Salt Wert ein Wörterbuch neu zu berechnen. Weicht man jedoch von der Variante rein in eine „Einweg-Hashfunktion und fertig“ ab und macht die Berechnung teuer, indem man sie zeitaufwendig gestaltet, wird diese Berechnung uninteressant bzw. unmöglich. Des Weiteren wird so erreicht, dass unabhängig von der Länge des Nutzerpasswortes (das, was Sie einegeben) immer die für AES (256 BIT) optimale Schlüssellänge vorliegt.

6. Das Programm sollte im Passwort Dialog ausreichend **vor der Eingabe „schlechter“ Passwörter schützen**.
   [Für Interessierte: *ArchiCrypt Passwort Safe setzt neben diversen mathematischen Verfahren eine 26 Mio. Einträge umfassende Datenbank ein (siehe oben), um durch die Bloom Filtering Methode die Eingabe bekannter Begriffe zu verhindern*]
7. Die Daten sollten bei geladenem Passwort Safe **im Hauptspeicher** durch einen bei jedem Start **zufällig erzeugten Sitzungsschlüssel verschlüsselt** werden.
8. Das **Programm** sollte **etabliert** sein, der **Anbieter** sollte **bekannt** sein.
9. Das **Programm** (*Installation und Anwendung*) sollte **digital signiert** sein, um Herkunft und Authentizität zu gewährleisten.

Nach diesen Artikeln sollten wir Folgendes mitgenommen haben!

Sofern man die Grundregeln bei der Passworterzeugung berücksichtigt und für jede Gelegenheit ein eigenes Passwort verwendet, hat man seine Risiken extrem minimiert. Zur Verwaltung der Passwörter, sollte man ein geeignetes Hilfsmittel wie zum Beispiel ArchiCrypt Passwort Safe nutzen.

