Einfaches Passwort mit 340 Bit

Helmut Schluderbacher, Peter Trykar

Merken Sie sich ein 50-stelliges Passwort?

Wohlgemerkt SIE SELBST, nicht Ihr Browser oder Passworttresor? Bestehend aus dem gesamten Zeichensatz, also Alphabet, Zahlen und 20 Sonderzeichen wild durcheinander gemischt? Oder merken Sie sich sogar einen 100-stelligen PIN? Nach, sagen wir mal, fünf Minuten lernen? Dann sind Sie ein Genie oder ein Mensch mit besonderen Fähigkeiten. Wenn Sie jedoch wissen wollen, wie das jede Person kann, dann lesen Sie weiter.

Das einzige, was Sie dazu tun müssen, ist, sich in 5 Minuten zwei von Ihnen ausgesuchte Bilder und vier von Ihnen dazu passend geknüpfte Assoziationen (gemeint sind Farben und/oder Formen) verinnerlichen zu können. Jedesmal, wenn Sie diese beiden Bilder sehen, sind auch die dazugehörigen Eigenschaften da. Jetzt sind Sie der perfekte Benutzer für ein neues grafisches Authentifizierungsverfahren namens SecLookOn, welches Sie beispielsweise zur Absicherung von Online Banking, Internetportalen und alle schützenswerten Transaktionen im Internet verwenden können. Ein Verfahren, dass derzeit zu den sichersten der Branche zählt, da es beim derzeitigen Stand der Technik weder abgehört oder sonstwie ausgehebelt werden kann. Ein Zuseher kann Hunderte SecLookOn-Anmeldevorgänge beobachten und wird trotzdem Ihre Kombination nicht erraten können.

Warum ist das so?

- SecLookOn ist eine Mischung aus **Steganografie** (so bezeichnet man die Möglichkeit Informationen in Bildern zu verstecken) und **Challenge/Response-Verfahren**, übersetzt bedeutet das in etwa Herausforderung-Antwort-Verfahren. Herkömmlichen Challenge/Response-Verfahren funktionieren nach folgenden Prinzipien: Der Teilnehmer muss nicht das Geheimnis (z.B. Passwort) übertragen, sondern er muss lediglich sicher beweisen, dass er das Geheimnis kennt. Er muss also auf eine gestellte Frage genau die dazu gehörige Antwort kennen. Um eine hohe Sicherheit zu gewährleisten, sind dabei jedoch einige Spielregeln einzuhalten:

- Es sollte sehr viele mögliche Antworten auf eine Frage geben.

- Ein Angreifer darf aus dem Zusammenfügen von Frage und Antwort nicht auf nachfolgende Antworten von nachfolgenden Fragen schließen können.

- Der Angreifer sollte schon die Frage nicht verstehen können.

Deswegen verwendet man Verfahren, bei denen das Wissen nicht preisgegeben werden muss, um herauszufinden, ob der andere Teilnehmer dies auch weiß.

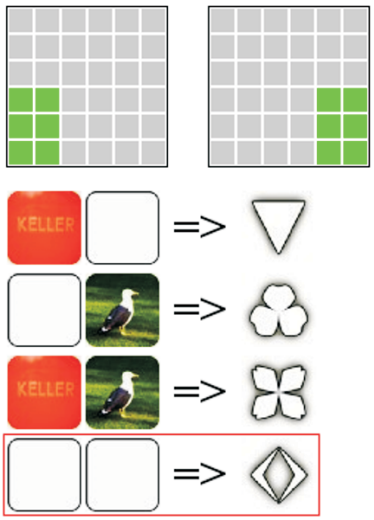
SecLookOn funktioniert nach einem ganz ähnlichen Schema. Jedoch werden dabei Bilder übertragen, und der wichtige Vorgang der Entschlüsselung findet alleine im Kopf des Benutzers statt. Erst nach dem Entschlüsseln der Kombination der Bilder gibt der Benutzer eine Zahl ein, die beweist, dass er das Geheimnis kennt. Diese Zahlen werden jeweils zufällig und immer wieder neu generiert, es entsteht ein so genannter Einmalkode. Im Normalfall müssen 4-5 Herausforderungen (Challenges) nacheinander gelöst werden, d.h. der Einmalkode ist 4-5 Stellen lang.

Wie funktioniert SecLookOn?

SecLookOn basiert auf zwei Bildern **(Bild rechts)**, links der Fotobereich und rechts der Eigenschaftsbereich. Diese Bilder sind in eine 6x6 Felder große Matrix unterteilt. In dieser Matrix sucht sich der Benutzer links und rechts sechs zusammenhängende Felder die sogenannte Gruppenauswahl aus, die dann seinen persönlichen Bereich ergeben. Die 30 übrigbleibenden Felder dienen dann nur mehr zur Verschleierung. Der nächste Schritt ist - wie bereits anfangs erwähnt - das Aussuchen von zwei Bildern; zwei Bilder, die den Benutzer ansprechen. In unserem Fall ist es das Bild Keller und das Bild Möwe. Nun kommt der wichtigste Teil der Aufgabe. Es geht darum, für den Benutzer richtige Assoziationen zu finden. In unserem Beispiel wird Keller mit dem Dreieck, Möwe mit dem Kleeblatt, wenn beide Bilder erscheinen mit dem Windrad und wenn keines der Bilder erscheint mit der Klammer assoziiert. Und damit ist auch schon die ganze Arbeit getan.

Es können natürlich auch andere Eigenschaften gewählt werden, z.B. Hintergrundfarben, die Farbe der Zahl oder des Symbols, spezielle Eckformen und so weiter. Alles in allem stehen in der Standard Edition bis zu 24 verschiedene direkt erkennbare Eigenschaften zur Verfügung. Diese können dann aber noch weiter verknüpft werden, so gibt es Verschiebungen, drei Bilder, Wiederholungen und vieles andere. In der Advanced Edition erreicht SecLookOn eine mögliche Sicherheit, die einem 340 Bit starken Schlüssel entspricht. Stellen Sie sich vor, sie behalten eine 1 mit 120 Stellen im Kopf, einfach so. Nach knapp fünf Minuten lernen.

Wie wir alle wissen, gibt es bei jedem Sicherheitssystem unterschiedliche Angriffsszenarien. SecLookOn bietet hier einige Abwehrmaßnahmen auf, die es wiederum einzigartig machen. So benötigt ein Mensch einen bestimmten Zeitraum, um auf die Challenge die richtige Response zu erkennen. Sollte diese



nun schneller als in einem definiertem Zeitraum erfolgen, dann nimmt das System automatisch an, dass nicht ein Mensch sondern ein Programm für die Eingabe sorgt. In diesem Fall wird die Eingabe nicht beachtet und verworfen. *Brute Force* Attacken können also nur mit der Geschwindigkeit eines Menschen erfolgen. Auch bei falschen Benutzernamen reagiert das System genau so, als gäbe es den Benutzer und stellt die Challenge. Einen korrekten SecLookOn-Schlüssel und damit eine korrekte Eingabe gibt es allerdings nicht dafür.

Wenn man sich als korrekter Benutzer bei der Eingabe irrt, kommt nach Abschluss aller Eingaben natürlich eine Fehlmeldung. Dies führt jedoch auch dazu, dass beim nächsten Anmeldevorgang zusätzliche Challenges beantwortet werden müssen. Bis zu 10 Durchgänge sind dabei möglich, wodurch sich die Sicherheit dramatisch erhöht. Ein angenehmer Nebeneffekt: der rechtmäßige Benutzer bemerkt, dass jemand versucht hat sich mit seiner Benutzerkennung anzumelden.

SecLookOn ist in zwei Editionen verfügbar, Standard und Advanced. Während die Standard Edition maximal 4 Eigenschaften und einen Replikationsserver bietet, bietet die Advanced Edition alle Sicherheitsmerkmale und Eigenschaften. Auch die Lizensierung ist zweigeteilt, es gibt die Möglichkeit, nach erfolgreichen Anmeldungen abzurechnen *„Pay per Use“* (Sehr interessant für Klein- und mittlere Betriebe, Schulen und Universitäten) und die herkömmliche Kauflizenz. Nähere Informationen über SecLookOn finden Sie im Internet auf www.seclookon.com oder direkt beim Hersteller MERLINnovations & Consulting GmbH.

Im linken Bildteil ist im persönlichen Feld die Möwe aber nicht der Keller sichtbar, daher ist das Kleeblatt gesucht: richtig ist daher 2