Station 4 – Passwörter

Hintergrund

Passwörter und geheime Schlüssel werden schon seit vielen Jahrhunderten eingesetzt. Auch die Zahl der Verschiebungen bei der Caesar-Verschlüsselung ist ein geheimer Schlüssel.

Im Laufe der Zeit ist die Komplexität der Schlüssel stark gestiegen. Von einer Ziffer, über gewöhnliche Wörter über Kombinationen aus Zahlen, Buchstaben, Sonderzeichen bis hin zu 4096 Bit langen Schlüsseln aus Nullen und Einsen.

Dem Schlüssel kommt nach dem Kerckhoffs'sche Prinzip eine besondere Rolle in der Kryptografie zu. Das Prinzip besagt, dass die Sicherheit einer Verschlüsselung nur von der Geheimhaltung des Schlüssels, nicht aber des Verfahrens abhängen darf. D.h. ein gutes Verschlüsselungsverfahren ist auch dann sicher, wenn eine dritte Person weiß, welches System wir einsetzten. Trotzdem kann sie es nicht knacken. Daher ist es auch kein Problem, dass die Algorithmen öffentlich diskutiert und geprüft werden. Im Gegenteil. Wenn Algorithmen von vielen Expertinnen und Experten untersucht und ausprobiert werden, ist die Chance gut, dass Fehler früh gefunden werden.

Doch Schlüssel und Passwörter werden nicht nur für die Verschlüsselung sondern auch zur Anmeldung bei Diensten wie Video-/Musikstreaming, Spielen, Nachrichtenportalen, Socialmedia und mehr genutzt.

Daher sind sie für Angreiferinnen und Angreifer ein lohnendes Ziel.

Angriffe auf Passwörter

Es gibt viele Arten von Angriffen auf Passwörter. Wir stellen euch zwei grundlegende Kategorien von Angriffen vor.

Offlineangriffe

Es kommt vor, dass jemand eine verschlüsselte Datei in die Finger bekommt oder ein Onlinedienstleister gehackt wurde und so die Nutzerdatenbank erbeutet wurde. In diesen Fällen, kann ein Offlineangriff auf die Daten durchgeführt werden. Das ermöglicht den Angreifern, mit ihrer eigenen Hardware wie z.B. vielen Grafikkarten die Versuche, das Passwort zu erraten, zu beschleunigen.

Passwörter werden in der Regel nicht einfach im Klartext gespeichert, sondern nur ein Hashwert davon. Einen Hashwert kann man sich als eine Art Fingerabdruck vorstellen. Jeder Klartext hat einen anderen Fingerabdruck. Dieser wird mit einer Hashfunktion erstellt und hat je nach Hashfunktion eine feste Länge. Modernere Systeme speichern zusätzlich einen Zufallswert, der bei jedem Passworteintrag anders ist. Diesen Zufallswert nennt man Salt und wird dann bei der Berechnung mit verwendet. So haben zwei gleiche Passwörter mit unterschiedlichem Salt trotzdem einen anderen Fingerabdruck.

Offlineangriffe werden dann gegen erbeutete gespeicherte Passwörter oder Daten durchgeführt. Dabei wird versucht, den Klartext für einen Hash zu finden.

Onlineangriffe

Bei Onlineangriffen, versucht sich eine Angreiferin oder ein Angreifer mit deinem Passwort an einem Dienst wie deinem Instagram-Account, oder Netflix anzumelden. Dabei werden nach und nach verschiedene Passörter durchprobiert.

Wenn der Betreiber des Dienstes seine Hausaufgaben gemacht hat, erkennt er den Versuch und unterbindet ihn, indem er z.B. den Account für fünf Minuten sperrt oder möchte, dass du einen Code aus einer SMS oder E-Mail eingibst.

Daher versuchen die Angreifer manchmal gar nicht einen Account mit vielen Passwörtern durchzuprobieren, sondern sie versuchen viele verschiedene Accounts mit einem Standardpasswort wie 123456 und schauen, ob irgendjemand so ein schlechtes Passwort verwendet hat.

Sicherheit von Passwörtern

Es gibt wahrscheinlich unzählige Regeln, wie man Passwörter aussuchen sollte. Es soll aus Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen bestehen und dann noch mindestens 12 Zeichen lang sein und keine Wörter, Namen oder Daten beinhalten. Und dann soll man für jeden Dienst auch noch ein anderes verwenden. Ganz schön schwierig.

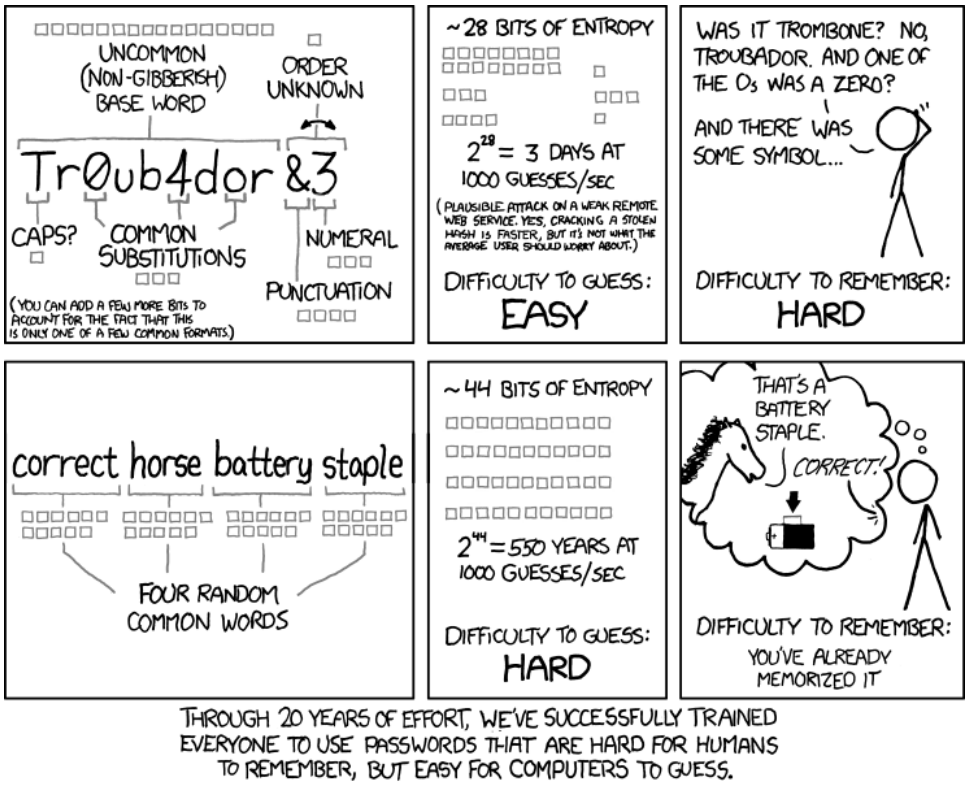
Doch warum gibt es diese Regeln eigentlich und welche Auswirkung haben sie auf die Sicherheit?

Mit dem Onlinetool passwordmonster können wir ausprobieren, welchen Einfluss die verschiedenen Regeln auf die Zeit hat, bis das Password geknackt werden kann. Aber bitte gebt nie eure echten Passwörter ein.

Ihr werdet sehen, dass Passwörter eigentlich für Menschen schlecht zu merken sind.

Passsätze

Als Alternative bieten sich Passätze an. Dabei wird nicht ein sehr komplexes, sondern ein einfaches, aber langes Passwort gewählt, das aus mehreren Wörtern besteht. Daher der Name Passsatz oder Passphrase. Ein bekannter Webcomic hat das schön zusammengefasst.



Quelle: XKCD - https://xkcd.com/936

Passwortmanager

Da sich das Merken von Passwörtern so schwierig gestaltet, bietet es sich an, einen Passwortmanager zu verwenden. Dabei braucht man sich nur ein langes, sicheres Passwort oder einen Passsatz zu merken, das den Manager entsperrt. Dieser generiert und speichert sichere Passwörter für die verschiedenen Dienste. Da die zufällig und lang sind, kann man sie sich nicht merken, aber das muss man auch nicht mehr. Denn der Passwortmanager merkt sie sich.

Ausprobieren

Wir haben zwei Seiten für Passwörter ausgewählt. Mit Passwordmonster kannst du erleben, welchen Einfluss die verschiedenen Passwortregeln wie Länge oder Sonderzeichen auf das Knacken des Passworts haben. Das Passwordgame treibt die Regeln für Passwörter auf die Spitze und stellt dir immer neue Herausforderungen. Mit den Hashtools kannst du ausprobieren, wie leicht oder schwer einfache Passwörter aus Hashes abgeleitet werden können.

Passwortkomplexität und -länge

Gehe im Browser auf https://www.passwordmonster.com/ und versuche folgende Passwörter. Überlege vorher, wie lange ein Computer wohl brauchen könnte, bis er das Passwort geknackt hat.

1. test1234
2. Test12345!
3. qwertzuiop!
4. 1?fBa3Ls"0
5. This_is_a_long_passhrase_without_strange_numbers_or_symbols

Wie gut waren deine Schätzungen?

Passwordgame

Gehe im Browser auf https://neal.fun/password-game/ und versuche möglichst viele der Regeln umzusetzen. Die Aufgaben werden mit der Zeit immer schwieriger. Wie weit schaffst du es?

Hashes

Erstelle dir für die folgenden Passwörter je einen MD5 Hash auf https://www.md5hashgenerator.com/ und füge ihn auf https://hashes.com/en/decrypt/hash ein. Was ist deine Vermutung, welche Passwörter er gleich berechnen kann und welche nicht?

1. 1234
2. test
3. test1234
4. Test12345!
5. qwertzuiop!
6. 1?fBa3Ls"0
7. This_is_a_long_passhrase_without_strange_numbers_or_symbols