Passwortsicherheit

Fachschaft Japanologie, Universität zu Köln

Gregor Billing

gbilling@smail.uni-koeln.de

11. Juni 2020

Einleitung

Passwörter sind das gängigste Authentifizierungsverfahren im Internet. Gleichzeitig ist ein Passwort oft auch die einzige Hürde, die ein Angreifer überwinden muss um Zugang zu sensiblen Daten zu erhalten. Zur Vermeidung solcher unbefugten Zugriffe muss dieses Passwort möglichst sicher gewählt werden.

Im folgenden wird daher ein gängiges Verfahren vorgestellt, um Passwörter sicher zu wählen und zu kommunizieren.

Inhaltsverzeichnis

1 Wahl eines Passworts

Dem Wortsinn nach handelt es sich bei einem „Passwort“ um ein *Wort*, mit welchem eine Zugangskontrolle *passiert* wird. Im Zeitalter des Internets ist jedoch ein einzelnes Wort kaum mehr genug, um Angreifer davon abzuhalten, Schaden anzurichten.

1.1 Level -1: Einzelne Wörter

Leider noch zu häufig Verwendung findet die Vergabe von einzelnen Begriffen oder Namen als Passwort für einen zu schützenden Bereich.

(1) `geheimnis`

Gängige Passwort-Cracker beginnen oft damit, bevor irgendwelche „schwarze Magie“ mit Kombinatorik betrieben wird, zunächst einmal stumpf den ganzen Duden / Oxford / Morohashi von vorne bis hinten durchzuprobieren. An dieser Stelle bricht unser Passwort-Schutz auf Level -1.

1.2 Level 0: Mehrere Wörter / Satz

Eine erste Verbesserung bietet die Vergabe eines aus mehreren Wörtern (oft aus Bequemlichkeit ohne die Verwendung von Leer- oder Satzzeichen) zusammengesetztes Passwort.

(2) `dasisteingeheimespasswort`

Leider sind moderne Rechner auch hier in der Lage, mithilfe einsprachiger Wörterbücher vergleichsweise schnell die Kombinationen aus bis zu 10 Wörtern zu probieren. Das hinzufügen von Satzzeichen bietet darüber hinaus auch nur geringfügig mehr Schutz – an dieser Stelle bricht unser Passwort-Schutz auf Level 0.

1.3 Level 1: Pseudo-randomisierte Buchstabensuppe

Die Sicherheit eines Satzes als Passwort kann erheblich gesteigert werden, wenn der Satz **unter Berücksichtigung von Satzzeichen** auf seine Anfangsbuchstaben reduziert wird. Das Passwort sieht also nach außen hin *scheinbar* zufällig aus, hat aber einen inhärenten Sinn für den Nutzer.

(3) `diegP`

Ab dieser Stelle ist ein Angreifer gezwungen, mit „roher Gewalt“ einfach zu raten, bis er zufällig euer Passwort trifft. Anbetrachts moderner Prozessoren und deren hoher Rechenleistung ist solch ein Vorgehen bis circa (!) 12 Zeichen Länge jedoch trivial. Ein Passwort auf Level 1 bietet also nur sinnvollen Schutz ab circa 15 Zeichen. Ein so komplex gewählter Satz kann jedoch schwierig zu merken sein.

Bonus: Beachtung von Groß- und Kleinschreibung ist hier sehr sinnvoll, da für den Computer `AbC` ein komplett anderes Passwort ist als `abc`. Die Einhaltung geltender Rechtschreibregeln generiert euch also „gratis“ mehr Zufall.

1.4 Level 2: Anreichern eines vorhandenen Passworts

Existierende Level-1-Passwörter können mit einer Art *Lückenfüllern* angereichert werden, um die Komplexität zu steigern ohne den Merkaufwand wesentlich zu erhöhen.

Dabei werden zwischen den Buchstaben des Passworts zusätzlich Zahlen eingefügt, die einem beliebigen Muster folgen. Dieses Muster sollte jedoch nicht zu vorhersehbar (1-2-3-4-usw.) gewählt sein, sondern idealerweise gar kein von außen erkennbares Schema haben (Postleitzahl eures Geburtsortes, TTMMJJJJ des Geburtsdatums eines Elternteils, etc.)

(4) `d1i1e2g3P5d8s13z21k34i`

Ab Level 2 kann mit einem hinreichend lang gewählten Satz davon ausgegangen werden, dass euer Passwort sicher ist. Mit anderen Worten: Wenn diese Art von Passwort geknackt wird, war es wirklich nicht eure Schuld und der Dienst der das Passwort speichert (um es bei jedem Login wieder überprüfen zu können) hat Mist gebaut.

1.5 Level 2+: Verwendung von Symbolen und Zahlen

Den höchsten trivial merkbaren Sicherheitsgrad bieten Level-2-Passwörter, die zusätzlich mit Symbolen versehen sind. Dabei genügt es im wesentlichen schon, einzelne Zahlen in eurer Level-2-Sequenz in Symbole zu verwenden. Aber auch andere Eselsbrücken, bei denen von vornherein eine Symbol-Sequenz statt einer Ziffer-Sequenz zum Anreichern gewählt wird, ist denkbar.

(5) `d1i1€2g3P5d8s!3z2!k34i`

Tipp: Das Drücken der Shift-Taste konvertiert auf den meisten gängigen Tastaturen jede Zahl in ein eindeutiges Symbol, kann jedoch zu Verwirrung bei unterschiedlichen Tastatur-Layouts führen.

Achtung: Nur das Zusammenspiel aus Ziffern *und* Symbolen erhöht die Sicherheit gegenüber Level 2. Wenn die Ziffern-Sequenz von Level 2 durchgängig mittels Shift in eine reine Symbolkette verwandelt wird, habt ihr effektiv auch nur ein Level-2-Passwort mit „komischen“ Zahlen generiert.

1.6 Level 3: Zusammenspiel mit Zwei-Faktor-Authentifizierung

Effektiv uneinnehmbar wird euer Account (bis auf gravierende Fehler seitens des Dienstes, bei dem euer Passwort hinterlegt ist), wenn ihr ihn um eine *Zwei-Faktor-Authentifizierung* (kurz 2FA) ergänzt. Dabei wird nach jeder erfolgreichen Passwort-Eingabe ein Code an euer Handy oder einen Online-TAN-Generator gesendet, der jeweils nur 30 Sekunden lang gültig ist und den ihr zusätzlich korrekt eingeben müsst um Zugriff auf den passwortgeschützten Bereich zu erlangen.

Leider unterstützen nicht alle Webseiten diese Art von zusätzlichem Sicherheitsmechanismus, aber falls er verfügbar ist solltet ihr dringend über ihren Einsatz nachdenken.

Bonus: Für extrem kritische Systeme kann man sich sogar *physische* Geräte bestellen, die aussehen wie ein USB-Stick und als zweiter Faktor fungieren. Bei jedem Login

muss dann der entsprechende Security Token in den USB-Port des Rechners eingesteckt werden, um die Anmeldung zusätzlich zum Passwort zu legitimieren.

TL;DR

Ein gutes Passwort⋯

- ⋯darf nichts enthalten, was in Wörterbüchern / Lexika / Enzyklopädien zu finden ist
- ⋯muss nach außen hin (scheinbar) zufällig zusammengewürfelt wirken
- ⋯sollte möglichst alle verschiedenen Zeichenklassen (GROSSBUCHSTABEN, kleinbuchstaben, 21ff3rn, $ond € rz € !ch € n) enthalten.

1.7 Alternative: Muster-basierte Passwörter

Die zuvor skizzierte Struktur, nach der ein Passwort mit mehreren Levels aufgebaut wird, ist nur eine Möglichkeit um sichere Passwörter zu erzeugen. Eine mögliche Alternative ist es, sich ein bestimmtes *Muster* auf der Tastatur einzuprägen (zwei Tasten hoch, drei Tasten links, Shift, eine Taste rechts, usw.) und ausgehend von einem bestimmten Ausgangsbuchstaben abzulaufen. Wenn der „Rand“ der Tastatur erreicht wird, zählt man von der gegenüberliegenden Seite weiter (Q + 2 links = Ü, Y + 3 unten = A).

Dadurch reduziert man das Passwort effektiv auf die Information, bei welchem Buchstaben das Muster jeweils angefangen wird, und kann dieses Muster dann mit unterschiedlichen Anfangsbuchstaben für unterschiedliche Dienste verwenden. Dieses System ist jedoch fehleranfällig bezüglich verschiedener Tastaturlayouts (beispielsweise vertauschtes Z/Y auf amerikanischen Tastaturen).

2 Kommunikation von Passwörtern

Sobald einmal ein sicheres Passwort vergeben wurde, muss es gegebenenfalls mit anderen Teilnehmern geteilt werden um zum Beispiel den Zugriff auf eine geteilte Datei zu ermöglichen. Dabei lautet die erste und wichtigste Grundregel: **Niemals Passwörter im Klartext kommunizieren, auch nicht über einen vermeintlich sicheren Kanal**. Das umfasst insbesondere auch die Notiz auf Papier oder in Tagebüchern!

2.1 Meta-Kommunikation

Passwörter werden am besten geteilt, indem man auf Meta-Ebene Informationen über das Passwort mitteilt, also dem griechischen Wortsinn nach *über* das Passwort spricht ohne es konkret zu erwähnen.

Bei Vergabe eines Level-2-Passwortes nach obigem Schema kann man zum Beispiel die Information (also meistens den Satz) austauschen, mithilfe derer das Passwort erzeugt wurde. Dabei sollte man sich zuvor auf eine Information festlegen, die der Gesprächspartner sicher besitzt, die aber auch nicht trivial ist.

2.1.1 Schlechtes Beispiel

Max Müller möchte ein Passwort mit Erika Meier teilen. Er generiert nach obigem Schema und dem Satz „Ich heiße Max Müller“ das Passwort `I1h2M3M`. Danach schreibt er Erika eine Nachricht: *Das Passwort besteht aus dem Satz mit dem ich mich einer unbekannten Person vorstelle. Verwende zwei Worte plus meinen Namen, und fülle die Lücken mit Ziffern in aufsteigender Reihenfolge.*

Falls jemand diese Nachricht abfängt, ist der Name dem Angreifer vermutlich schon bekannt, und die verwendete Ziffernfolge wird konkret erwähnt.

2.1.2 Akzeptables Beispiel

Max Müller möchte ein Passwort mit Erika Meier teilen. Er generiert nach obigem Schema und der Phrase „Dürener Straße, Köln Lindenthal“ das Passwort `d1s0,2k6l`. Danach schreibt er Erika eine Nachricht: *Das Passwort besteht aus dem Straßennamen und dem Namen von Stadt und Stadtteil in dem sich unser Institut befindet. Fülle die Lücken mit den Ziffern der Anzahl an Kanji die japanische Grundschüler lernen.*

Diese Informationen kann man im Zweifelsfall googeln, man muss aber wissen welches Institut gemeint ist und auch die Klassifikation „Stadtteil“ ist mehrdeutig. Wenn man den konkreten Begriff *Kyôiku-Kanji* nicht kennt, und auch sonst nicht weiß wie das japanische Schulsystem aufgebaut ist, ist zudem die Ziffernfolge nicht trivial rekonstruierbar.

2.1.3 Gutes Beispiel

Max Müller möchte ein Passwort mit Erika Meier teilen. Er generiert nach obigem Schema und der Phrase „ この小さい箱はどうしましょうか “ das Passwort

`k2n1c2i2s3i2h3k2h3d4u2s1m3s1y2u2k3`. Danach schreibt er Erika eine Nachricht: *Schlage das Japanisch-Lehrbuch für Erstsemester auf Seite 162 auf. Wähle den drittletzten Satz des Umzugshelfers, ersetze alle Kanji durch Kana und wähle dann von jedem Kana den Anfangsbuchstaben in Hepburn-Umschrift. Füge nach jedem einzelnen Buchstaben jeweils die Strichzahl des Kanas ein.*

Um dieses Passwort zu erraten, braucht man zunächst das Kontext-Wissen welches Lehrbuch im ersten Semester verwendet wird, und muss es physisch besitzen. Darüber hinaus muss man der japanischen Sprache hinreichend mächtig sein, um die Fachinformationen rekonstruieren zu können.

2.2 Anmerkungen zur Kommunikation

Die oben skizzierten Beispiele sind jetzt „öffentlich“ und eignen sich daher nicht mehr als Schema für eigene Passwörter. Bei der Kommunikation sollte außerdem darauf geachtet werden, wer das Passwort im Zweifelsfall ausspionieren könnte – so ist das „gute“ Beispiel von eben zwar im Kontext des Internets insgesamt sehr sicher, hilft aber nichts wenn man die Kommunikation in einer Gruppe abhält in der lauter Japanologie-Studenten mitlesen. Daher gilt: Nicht möglichst kompliziert, sondern möglichst unintuitiv für mögliche Angreifer kommunizieren.

Ein weiterer, durchaus wertvoller Weg zur Kommunikation ist die persönliche Kommunikation in Präsenz. Das bedeutet, dass man durchaus auch direkt ein Passwort benennen und gemeinsam ein Passwort wählen kann, wenn man sich im selben Raum befindet und außerhalb der Hörweite anderer Menschen spricht.

3 Schlussbemerkung

Letztendlich ist ein gutes Passwort nur ein Glied in der Kette, und gute Sicherheit steht und fällt damit ob die lange Kette als ganzes hält. Sichert also immer zuerst das schwächste Glied - das ist in den meisten Fällen euer E-Mail-Konto (falls ein Angreifer in euren Mail-Account eindringt kann er sich mit der *Passwort vergessen?*-Funktion Zugriff zu quasi jedem anderen Internet-Account verschaffen).

Nutzt einen Passwort-Manager wenn ihr könnt. Gebt euch Mühe ein möglichst sicheres Master-Passwort zu generieren, das den gesamten Tresor verschlüsselt, und lasst den Passwort-Manager dann die restliche Arbeit machen. Diese Programme können auch tatsächlich zufällige Zeichenketten für euch generieren, dann braucht ihr diese nur noch per Copy/Paste einzufügen und in eurem Tresor zu speichern, ohne euch das einzelne Passwort konkret merken zu müssen.