Untersuchung zur Merkbarkeit von Passwörtern mit Hilfe von Bildern

# Motivation

Der Zugang zu Informationssystemen wird typischerweise mit einem Passwort abgesichert. Auch wenn biometrische oder Hardware-basierte Verfahren ergänzend oder ersetzend verwendet werden, wird den Passwörtern auch weiterhin eine wichtige Bedeutung beigemessen, um Zugriffe abzusichern.

Je nach Zugriffsmöglichkeit auf ein IT-System empfiehlt das BSI für Passwörter eine Länge von 12 Zeichen, bestehend aus zufälligen Zeichen. Diese Zeichen sollen sowohl Groß- und Kleinbuchstaben, Ziffern als auch Sonderzeichen enthalten. Dies stellt hohe Anforderungen an die Merkfähigkeit der Nutzer. Hier kann man sich Eselsbrücken bauen und zum Beispiel die Anfangsbuchstaben der Worte eines Satzes nehmen und diese Zeichenfolge durch Ziffern und Sonderzeichen ergänzen. Hierbei ist es allerdings unwahrscheinlich, dass bei einem selbst gewählten Passwort alle Zeichen gleich wahrscheinlich sind.

Eselsbrücken sind eine gute Merkhilfe. Hierbei werden scheinbar zufällige oder schwer zu verknüpfende Informationen mit leicht zu merkenden Informationen des alltäglichen Lebens verknüpft, wie vom BSI empfohlen <https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2011/Passwortsicherheit_27012011.html>

Ziel des Tools ist es, mögliche Aussagesätze von Vorgängen in Passwörter umzusetzen. Der Nutzen beruht auf der Annahme, dass der Mensch sich Vorgänge oder Geschichten wesentlich besser merken kann als abstrakte Symbole. (Nachweis fehlt noch) Diese Passwörter decken den gesamten Zustandsraum der möglichen Zeichen ab. Auch Muster kann man sich besser merken

Das Tool soll den Anforderungen des IT-Grundschutze zur Speicherung von Passworten entsprechen <https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04306.html?nn=6610630>  entsprechen, obwohl kein Passwort gespeichert wird.

# Anforderungen

Die Anforderungen werden unterteilt in funktionale und nicht-funktionale Anforderungen.

## Funktionale Anforderungen

Die funktionalen Anforderungen werden als Anwendungsfälle dargestellt:

### App zum Passwort-Gedächtnistraining

Das Tool soll folgende Funktionsmerkmale (Use Cases) enthalten:

1. Der Nutzer kann eine Sequenz aus in Bildern und textuell dargestellten Begriffen eingeben. Dadurch entsteht eine vermutlich leichter merkbare Sequenz von Begriffen als eine Art Handlung.
2. Im Anschluss an die Eingabe werden die Begriffe dem Nutzer grafisch und textuell dargestellt. Die textuelle Darstellung soll in der Art einer Aussage in Textform dargestellt werden. Dies muss nicht grammatikalisch korrekt sein.
3. Die Sequenz wird mit dem Bezeichner persistent im Gerät gespeichert.
4. Aus dieser Sequenz kann unter Berücksichtigung einer konfigurierbaren Passwort-Policy ein rein textbasierte Passwort generiert werden.
5. Optional: Der Nutzer kann für die Genrierung von textuellen Passwörtern für jedes Passwort eine PIN-Policy festlegen.
6. Die PIN-Policy besteht aus der Möglichkeit der Wahl des Einbeziehens oder Ausschließens von folgenden Zeichen:
   1. Kleinbuchstaben
   2. Großbuchstaben
   3. Ziffern
   4. Sonderzeichen
7. Das jeweils eingegebene Passwort kann mit einem Bezeichner, wiz.B. „HfTL-Email“ versehen werden.
8. In konfigurierbaren Zeitintervallen wird das Passwort geübt. Z.B. 1,2,4,7,14,30,60, 180 Tage. Bei Erfolg wird das Wiederholintervall verlängert, bei Misserfolg am nächsten Tag wiederholt und auf das nächstkürzere Intervall gesetzt.
9. Optional: Triviale Passworte werden erkannt und nicht zugelassen.
10. Passworte und dazugehörige Bildsequenzen können auch vom System mit Hilfe eines Pseudozufallsgenerators erzeugt werden.
11. Ereignisse des Trainierens eines Passworts werden persistent im Gerät gespeichert und mit einer Server-Applikation synchronisiert.
12. Statistische Daten über die mittlere Merkfähigkeit aller Nutzer werden im Vergleich zum jeweiligen Nutzer angezeigt.
13. Die statistischen Daten werden aufgeschlüsselt nach
    1. Art des Passworts: Handlungssequenz mit Bild und Text oder Zeichenkette
    2. Art der Erzeugung des Passworts: Selbst erstellt oder per Pseudozufallsgenerator erzeugt.

### Server-Applikation

1. Die Server-Applikation speichert persistent Daten der verschieden Instanzen einer App.
2. Die Server-Applikation stellt für das Speichern und Abrufen von Daten eine Schnittstelle zur Verfügung.
3. Im upload werden nur Daten eines Nutzers bezüglich der Wiederhol-Tests gespeichert.
4. Im Download werden ausschließlich die eigenen oder statistische Daten über alle Nutzer oder Nutzergruppen zur Verfügung gestellt.

## Nicht-Funktionale Anforderungen

### App zum Passwort-Gedächtnistraining

### Server-Applikation

1. Die Server-Applikation speichert persistent Daten der verschieden Instanzen einer App.
2. Hierzu wird ein möglichst einfaches Kommunikationsprotokoll und Datenformat benutzt.
3. Optional: Jede Instanz einer App registriert sich beim Erstzugriff am Server tauscht Authentifizierungsdaten für den weiteren Zugriff aus. Dies geschieht wie folgt:
4. Generierung einer gerätespezifischen DeviceID
5. Übertragung der DeviceID vom Gerät an den Server über eine abhörsichere Verbindung.
6. Übertragung der ServerID vom Server an das Gerät über eine abhörsichere Verbindung.
7. Optional: Bei der Anmeldung wird mittels eines Challenge-Response-Verfahrens eine Authentifizierung durchgeführt und eine authentifizierte Sitzung erstellt.

*Kommentar: Was benutzt Firebase zur Authentifizierung?*

1. **Passwort-App**

-Übernahme eines fertigen Passwortes in die Zwischenablage

-Löschen der Zwischenablage nach einem angemessenen Zeitraum

**Technische Umsetzung**

**Algorithmen**

**Passwort-Erzeugung**

Algorithmus für Erzeugung eines Passwortes mit den zeichen Z[0] .. p[n] aus der Liste mit Eingaben e[0]..e[S] mit e[i] in {0..N}

Annahme N= 19, S=11

1. Erzeugung der Passwort Number PN:

PN =

1. Erzeugung von Zeichen aus dem Zeichensatz Z[M] gemäß Passwort Policy. Die Anzahl  M ergibt sich aus der Passwort-Policy. So ist M zum Beispiel für [A\_Za\_z0\_9!"§$%&/()=] entsprechend 72

Q[0] = PN

Z[i] = Q[i] mod M

Q[i+1] = Q[i] div M

1. Der Algorithmus endet wenn Q[i]  nur noch 0 ergibt.

Überschlagsrechnung

4x5 Elemente in 10 Dialogen = 10^13

Äquivalent zu 13 Ziffern oder 7 Zeichen (52+10Ziffern+10 Sonderzeichen)

BSI-Empfehlung 12 Zeichen = 1,94 \* 10^22 - 17 Dialoge erforderlich

Bzw. 8 Zeichen 1,7 \*10^15 - 12 Dialoge erforderlich

**Passwort-Eingabe**

Die in der Abfolge angezeigten Bilder  lassen sich leichter merken, wenn man diese in einen Zusammenhang bringen kann. Dieser Zusammenhang kann eine Folge von Geschehnissen oder ein Handlungsablauf sein. Ein Handlungsablauf lässt sich in folgenden  Teilen formal darstellen:

Subjekt, Prädikat, temporale adverbiale Bestimmung, lokale adverbiale Bestimmung, Ort

Folgende Bildsequenzen sind grundsätzlich denkbar:

1. Subjekt

Mann, Frau, Baum, Katze, Hund, Auto, Ball, Pferd, Mädchen, Junge, LKW, Fahrrad, Motorrad, Busch, Käfer, Polizist, Feuerwehrmann, Bauarbeiter, Pferd, Kuh, Schaf,

1. Prädikat

geht

Läuft

Rennt

Springt

Tanzt

Liegt

Rollt

schaut

Rast

Isst

Schläft

Steht

Fällt hin

Steigt hinauf

Steigt hinab

Träumt

Trinkt

Riecht

bleibt

duftet

1. Nähere Beschreibung Prädikat - zeitlich

Nie

Selten

manchmal

oft

Immer

Am Morgen

Am Mittag

Am Nachmittag

Am Abend

In der Nacht

Am Wochenende

bei Winter

bei Sommer

bei Herbst

bei Regen

bei Sonnenschein

bei Nebel

bei Gewitter

bei Schnee

bei Wind

1. Nähere Beschreibung Ort

Riesig

Groß

Klein

Winzig

Lang

Breit

Hoch

Sauber

Schmutzig

Flach

Rund

Eckig

Oval

Schräg

Violett

Grau

Rosa

Bunt

Alt

neu

1. Ort

Strand

Wiese

Straße

Autobahn

Fußweg

Himmel

Erde

Wald

Garten

Feld

Supermarkt//Gebäude

Einfamilienhaus

Villa

Schloss

Bahnhof

Bach//Gewässer

Fluss

Teich

See

Meer