Alexander Schmiedl, Nils Steinlein, Nastassia Vysotskaya, Johannes Gasthuber, Paul Gerhart, Rümeysa Gel, Tobias Krieg

Human Factors in Security and Privacy

Übungsblatt 01

Aufgabe 1

Aufgabe 2 Passwortrichtlinien

2.1

Richtlinie A:
mögliche Zeichen: 26 [Kleinbuchstaben] + 10 [Ziffern] = 36
mögliche Passwortlängen: 8
Rechnung: $36^8 = 2,82 * 10^{12}$

Richtlinie B:
mögliche Zeichen: 26 [Kleinbuchstaben] + 10 [Ziffern] + 35 [Sonderzeichen] = 71
mögliche Passwortlängen: $10, 11, 12$
Rechnung: $71^{10} + 71^{11} + 71^{12} = 1,66 * 10^{22}$

Richtlinie C:
mögliche Zeichen: 26 [Kleinbuchstaben] + 26 [Großbuchstaben] + 10 [Ziffern] + 35 [Sonderzeichen] = 97
mögliche Passwortlängen: $6, 7, 8$
Rechnung: $97^6 + 97^7 + 97^8 = 7,92 * 10^{15}$

2.2

Passwörter pro Sekunde als Zehnerpotenz: 100 Millionen = 10^8

Durch die Vereinfachungen ergeben sich:

- $3 * 10^{12}$ mögliche Passwörter für Richtlinie A:

$$\frac{3*10^{12}}{10^8} \frac{PW}{PW\ pro\ Sekunde} = 3 * 10^4 Sekunden = 8,33\ Stunden \quad \big) : 3600\ Sekunden/Stunde$$

- $1.5 * 10^{22}$ mögliche Passwörter für Richtlinie B:

$$\begin{aligned} \frac{1.5*10^{22}}{10^8} \frac{PW}{PW\ pro\ Sekunde} &= 1.5 * 10^{14}\ Sekunden && \big) : 3600\ Sekunden/Stunde \\ &= 4,166 * 10^{10}\ Stunden && \big) : 24\ Stunden/Tag \\ &= 1736111111\ Tage && \big) : 365\ Tage/Jahr \\ &= 4756468,798\ Jahre \\ &= 4,76 * 10^6\ Jahre \end{aligned}$$

- $8 * 10^{15}$ mögliche Passwörter für Richtlinie C:

$$\begin{aligned}
\frac{8*10^{15}}{10^8}\frac{PW}{PW\ pro\ Sekunde} &= 8*10^7\ Sekunden && \big)\ : 3600\ Sekunden/Stunde\\
&= 22222,2222\ Stunden && \big)\ : 24\ Stunden/Tag\\
&= 925,93\ Tage && \big)\ : 365\ Tage/Jahr\\
&= 2,54\ Jahre\\
&= 2,54*10^0\ Jahre\\
&= 0,254*10^1\ Jahre
\end{aligned}$$

2.3

Durch die Vereinfachungen ergeben sich:

- $3*10^{12}$ mögliche Passwörter für Richtlinie A:

$$\begin{aligned}
3*10^{12}\ PW*256\ Bits\ pro\ PW &= 7,68*10^{14}\ Bits && \big)\ :8\ Bits/Byte\\
&= 9,6*10^13\ Byte && \big)\ : 10^{12}\ Byte/Terabyte\\
&= 96*10^0\ Terabyte
\end{aligned}$$

- $1.5*10^{22}$ mögliche Passwörter für Richtlinie B:

$$\begin{aligned}
1.5*10^{22}\ PW*256\ Bits\ pro\ PW &= 3,84*10^{24}\ Bits && \big)\ :8\ Bits/Byte\\
&= 4,8*10^{23}\ Byte && \big)\ : 10^{12}\ Byte/Terabyte\\
&= 4,8*10^{11}\ Terabyte
\end{aligned}$$

- $8*10^{15}$ mögliche Passwörter für Richtlinie C:

$$\begin{aligned}
8*10^{15}\ PW*256\ Bits\ pro\ PW &= 2,048*10^{18}\ Bits && \big)\ :8\ Bits/Byte\\
&= 2,56*10^{17}\ Byte && \big)\ : 10^{12}\ Byte/Terabyte\\
&= 256000\ Terabyte\\
&= 2,56*10^5\ Terabyte
\end{aligned}$$

2.4

Wenn man für eine Webseite zwischen Richtlinie A und C entscheiden müsste, würden wir Richtlinie C empfehlen. Da diese alle Zeichen erlaubt und nicht eine exakte Länge, sondern eine innerhalb eines Längenintervall verlangt, ist dies die benutzerfreundlichere Variante – gerade im kommerziellen Bereich, wo die Konkurrenz groß ist, ist dies ein wichtiger Aspekt. Auch vom Sicherheitsstandpunkt ist C besser, da hier die Zahl möglicher Passwörter größer ist.

2.5

Usability:
Die Usability von Richtlinie C ist vermutlich die beste, da User nicht eingeschränkt, was die Wahl ihrer Zeichen innerhalb des gesetzten Passworts angeht – weder Richtlinien A, noch B erlauben die Nutzung von Großbuchstaben. Zudem ist man bei der Richtlinie C etwas flexibler, was die Zeichenkettenlänge betrifft, da sie zwischen 6 und 8 liegen kann und sie in Richtlinie A fix bei 8 liegt. Richtlinie B hat zwar auch einen Toleranzbereich von 10 bis 12 Zeichen, allerdings ist eine kürzere Zeichenkette einfacher zu merken und verringert so unter Umständen das Risiko, das Passwort zu vergessen. Allerdings muss zu allen Richtlinien gesagt werden, dass sie alle eine zu geringe Maximallänge erlauben, da längere Passwörter, welche allerdings leicht einprägbar sind, nicht erlaubt sind.

Security: Richtlinie A scheint die am wenigsten sichere Richtlinie zu sein, da nur Kleinbuchstaben und Ziffern verwendet werden dürfen und die Länge auf genau 8 Zeichen festgelegt wird. Dies erleichtert selbstverständlich offline Attacken wie Brute-Force oder Dictionary-Attacken, da sie auch die geringste Anzahl an möglichen Passwörtern aufweist. Richtlinie C erlaubt zwar die meisten möglichen Zeichen, allerdings sind hier sehr kurze Passwörter erlaubt von 6 bis 8 Zeichen, weshalb es aus Security-Sicht einen geringeren Status als Richtlinie B erreicht. Zwar werden hier keine Großbuchstaben erlaubt, allerdings tritt hier das Intervall mit der größten minimalen Länge hervor und auch die Längenvarianz ist (mit der von Richtlinie C) die größte. Dadurch und durch den Fakt, dass hierbei die größte Anzahl an möglichen Passwörtern existiert, ist sie besonders für offline-Attacken geschützt.
Natürlich existiert der bessere Schutz vor offline Attacken nur, wenn vom Provider Salted Hashing verwendet wird. Ansonsten schützt auch das "beste"Passwort nicht vor einem Angriff.

Zusätzliche Maßnahmen: Eine Möglichkeit wäre Blacklisting: Häufige/triviale Passwörter wie 12345678 oder etwa eine Zeichenkette, welche den Website-Namen inkludiert würden somit verboten. Dies erschwert Dictionary Attacken. Zudem könnte man beispielsweise verlangen, von jeder erlaubten Zeichengruppe mindestens eines im Passwort zu inkludieren und das Passwort nicht mit einer Zahl enden zu lassen.

2.6

Bezüglich der Usability bewerten wir dies als kreative Idee, dem Nutzer einen Leitfaden für ein gutes Passwort zu geben. Allerdings müsste man den Nutzer bei der Passworteingabe daran erinnern, dass er unter Umständen daran denken sollte, dass bei dieser Website eventuell ein Merksatz als Passwort-Basis diene. Ansonsten ist es wahrscheinlich, dass der Nutzer vergisst, auf welcher Seite er dazu aufgefordert wurde, sich einen Merksatz heranzuziehen und vergisst sein Passwort trotzdem.