Reduktion von Fehlerraten mittels ergonomischer Passwörter

David Weich · Britta Herres · Konstantin Knorr

Fachhochschule Trier
{weichd | herresb | knorr}@fh-trier.de

Zusammenfassung

Passwortgeneratoren erzeugen komplexe Passwörter, bei deren Eingabe Nutzer sich leicht vertippen. Dadurch wird die Akzeptanz solcher Passwörter reduziert. Wünschenswert sind Passwörter, die sich schnell und ohne Fehler eintippen lassen und gleichzeitig eine vorgegebene Komplexität aufweisen. Dazu wurden ein Softwareprototyp, das „Ergonomic Password Tool“ (EPT), entwickelt und die generierten Passwörter einem Praxistest unterzogen. Zunächst befassen wir uns mit dem gegenwärtigen Stand von Passwortgeneratoren, mit ergonomischen Betrachtungen des Tippverhaltens und mit statistischen Untersuchungen von Tippfehlern. Daraus werden Anforderungen zur Generierung ergonomischer Passwörter abgeleitet, die im EPT umgesetzt werden. Dabei wurden das Zehnfingersystem und die deutsche QWERTZ-Tastatur zugrunde gelegt. EPT wurde einem Praxistest unterzogen, der zeigte, dass die Fehlerraten mittels EPT erzeugter Passwörter im Verhältnis zu anderen allein sicherheitsorientierten Passwörtern um durchschnittlich 52 % reduziert werden und gleichzeitig die Anschlagraten um durchschnittlich 18 % höher liegen. Den Abschluss bildet eine Diskussion der Sicherheit und Merkbarkeit der ergonomischen Passwörter und möglicher Angriffe wie z.B. ein Angriff über ein EPT-Wörterbuch und ein Ausblick auf zukünftige Arbeiten.

1 Einleitung

Eine Aufgabe, die jedem Benutzer einer passwortgeschützten Anwendung begegnet, ist die der Erstellung eines Passwortes. Soll ein Passwort so gestaltet werden, dass es gängigen Sicherheitsanforderungen genügt, so werden diese Passwörter oft sehr komplex. Passwortgeneratoren, wie beispielsweise in *KeepPass* ([Kee]) enthalten, können Passwörter basierend auf Sicherheitsrichtlinien erzeugen, wie sie zum Beispiel vom *Bundesamt für Sicherheit in der Informationstechnik* ([BSI, Dat]) vorgestellt sind. Diese Passwörter erfüllen zwar die vom Benutzer eingestellten Vorgaben, jedoch lassen sich diese Passwörter oft weder schnell und fehlerfrei eintippen noch kann der Nutzer sich diese Passwörter merken [Ande08].

Wünschenswert wären Passwörter, die den folgenden drei Kriterien genügen:

- **Sicherheit:** Je nach Szenario wird z.B. die Einhaltung vorgegebener Passwort-Richtlinien, die Einhaltung einer gewissen Entropie oder Resistenz gegen Brute-Force-Angriffe gefordert.
- **Merkbarkeit:** Die Merkbarkeit sagt aus, wie leicht sich ein Anwender das Passwort merken kann. Sind Passwörter nicht merkbar, so werden diese vom Anwender nicht akzeptiert und häufig niedergeschrieben.
- **Ergonomie:** Übertragen auf die Eingabe von Passwörtern interpretieren wir die Ergono-

P. Schartner · J. Taeger (Hrsg.) · D•A•CH Security 2012 · syssec (2012) 389-399.

mie in diesem Beitrag als

a) die möglichst fehlerfreie Eingabe der Passwörter und
b) eine erhöhte Anschlagrate bei der Eingabe im Vergleich zu herkömmlichen Passwörtern.

Die Zielsetzung dieses Papiers ist es also, Passwörter zu erzeugen, die sich unter Berücksichtigung von Sicherheitsvorgaben möglichst fehlerfrei und schnell vom Anwender eingeben lassen.

Schwierig wird es, diese Kriterien in einem Passwort zu vereinen, da die einzelnen Kriterien negativ miteinander korreliert sein können. Ein Passwort, welches vollen Sicherheitsanforderungen genügt (z.B. einer komplexen Passwort-Richtlinie), ist mit hoher Wahrscheinlichkeit nicht schnell und fehlerfrei einzugeben. Dies folgt aus der Anforderung, dass Zeichen jedes Zeichenraumes in diesem Passwort enthalten sein sollen. Weiterhin ist die Sicherheit auch von der Länge des Passwortes abhängig. Mit jedem Zeichen steigt die Wahrscheinlichkeit von auftretenden Tippfehlern. Es ist zudem oft schwierig, sich ein sicheres Passwort aufgrund der Komplexität zu merken. Abbildung 1 verdeutlicht dieses Problem. Hier werden drei jeweils acht Zeichen lange Passwörter gegeneinander getestet. Die dargestellten Sicherheits- und Ergonomiewerte wurden aus dem entwickelten Ergonomic Password Tool (vgl. Kapitel 3) entnommen, die Merkbarkeitswerte sind geschätzt.

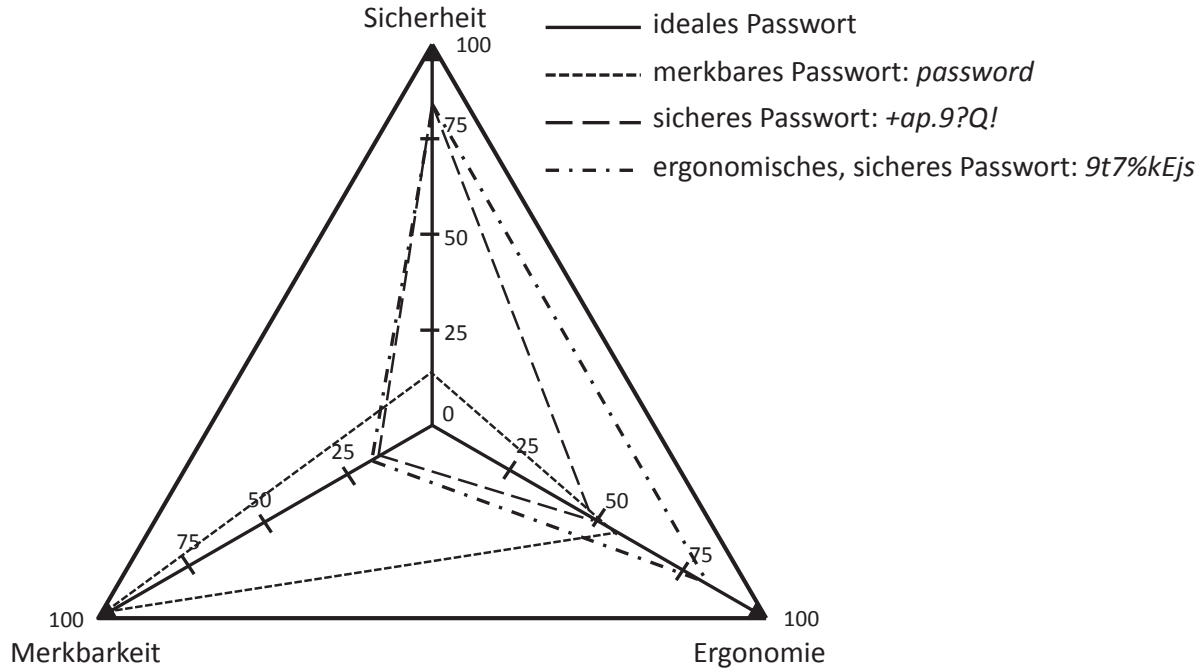

Abb. 1: Problematik der Wahl eines Passwortes bei Betrachtung der drei Kriterien

Studien wie [Cas] beschäftigen sich neben der Sicherheit mit dem Thema der Merkbarkeit von Passwörtern. Diese zielt jedoch nicht auf alphanumerische Passwörter ab, sondern beruht auf grafischen Passwortsystemen. Ross Anderson beschreibt in [Ande08] eine Nutzerstudie. Diese zeigt auf, wie Benutzer Passwörter wählen sollten, sodass sie merkbar, aber auch gleichzeitig sicher sind. Hierzu gehört die Verwendung von sogenannten *Passphrases*, wie sie auch in [Stam05] zu finden sind. Ein weiterer Vorschlag für merkbare Passwörter sind sogenannte

„Environ“-Passwörter [Ande08], die einem bestimmten Ablauf folgen, wie zum Beispiel bei acht Zeichen, die aufgeteilt sind in Konsonant, Vokal, zwei Konsonanten, Vokal, Konsonant und zwei Ziffern. Ein Beispiel ist „paspas12“. Ein anderer Ansatz zum Generieren merkbarer Passwörter ist in [Dic] beschrieben.

Zusammenfassend lässt sich sagen, dass Studien über Sicherheit und Merkbarkeit von Passwörtern vorhanden sind, die Ergonomie der Passwörter jedoch noch keinen Studien zugrunde liegt. Daher haben wir uns im Rahmen eines Bachelor-Teamprojektes an der Fachhochschule Trier mit diesem Thema beschäftigt [HeWe12].

Der Rest des vorliegenden Papiers hat die folgende Struktur: Zuerst werden die Anforderungen an ergonomische Passwörter in Abschnitt 2 aufgestellt. Diese werden anhand einer Statistik und Studien bezüglich des Tastaturlayouts belegt. Im Abschnitt 3 zeigen wir die Umsetzung der Anforderungen im Ergonomic Password Tool und stellen das Programm vor. Der Praxistest der ergonomisch generierten Passwörter im Vergleich zu rein sicherheitsorientierten Passwörtern wird in Abschnitt 4 vorgestellt und ausgewertet. Zusätzlich betrachten wir die Sicherheit und Merkbarkeit der EPT-Passwörter in Kapitel 5, bevor wir abschließend in Kapitel 6 das Resümee ziehen und auf zukünftige Arbeiten eingehen.

2 Anforderungen an ergonomische Passwörter

Grundlage unserer ergonomischen Betrachtung ist die deutsche QWERTZ-Tastatur nach DIN 2137 [DIN] und das Zehnfingersystem. Dieses ist nicht standardisiert, dennoch nutzen alle Schreibtrainer dieselbe Grundlage der Fingerbelegungen, wie sie in Abbildung 2 zu sehen ist.

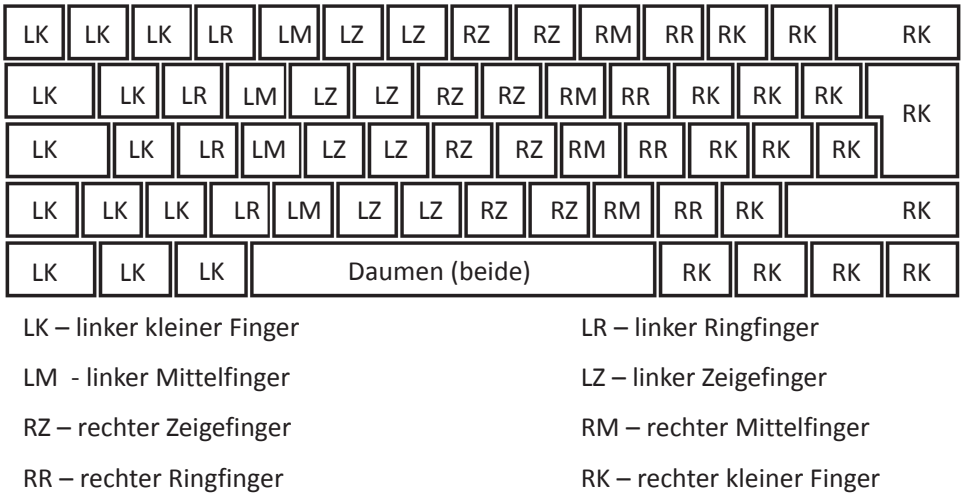

Abb. 2: Fingerbelegung der QWERTZ-Tastatur beim Zehnfingersystem

Tabelle 1 zeigt unsere Anforderungen an ergonomische Passwörter. Diese sind zum einen aus Dvoraks Thesen [JoMo88, Rohm82], zum anderen aus eigener Schreiberfahrung und der Analyse des QWERTZ-Layouts abgeleitet.

Die Anforderungen 1-3 werden durch die Arbeiten [JoMo88, NEO, Rohm82] belegt. Um die Thesen 4-8 zu prüfen, haben wir Probanden 30 deutsche und englische Texte an einer deutschen Standard-QWERTZ-Tastatur tippen lassen. Diese Texte boten nahezu den gesamten Zeichenraum der deutschen Sprache. Der Test wurde mithilfe des Schreibtrainers Tipp10 [TIP]

Tab. 1: Anforderungen an ergonomische Passwörter

Nummer	Anforderung	Belegt durch
1	Nach jedem getippten Buchstaben sollte ein Handwechsel erfolgen.	[JoMo88, Rohm82]
2	Ein Finger sollte keine „weiten Strecken“ auf der Tastatur zurücklegen.	[JoMo88, Rohm82]
3	Bei wiederholter Nutzung desselben Fingers sollten horizontale Bewegungen genutzt werden.	[JoMo88, Rohm82]
4	Ist es nicht möglich das Eingeben des Passwortes auf beide Hände gleich zu verteilen, sollte der Schwerpunkt auf der stärkeren Hand des Nutzers liegen.	[JoMo88, Rohm82]
5	Je näher die Finger am Daumen liegen, desto beweglicher und stärker werden sie. Ein kleiner Finger ist demnach nicht so beweglich wie ein Zeigefinger.	Statistik, Tabelle 2
6	Sonderzeichen sollten in zu generierenden Passwörtern den kleinsten Anteil einnehmen. Dabei gibt es eine Unterscheidung von normalen und Third-Level Sonderzeichen.	Statistik, Tabelle 2
7	Das Tippen von Großbuchstaben ist dem Tippen von Sonderzeichen zu bevorzugen.	Statistik, Tabelle 2
8	Zahlen sind nach Kleinbuchstaben der Zeichenraum, der beim Generieren der Passwörter zu bevorzugen ist.	Statistik, Tabelle 2

durchgeführt, so konnten Statistiken über Fehlerraten der einzelnen Zeichen extrahiert werden. Die Gesamtstatistik der einzelnen Finger und der Zeichen zeigt Tabelle 2. Mit Third-Level Sonderzeichen sind solche gemeint, die mit *AltGr* getippt werden. Diese zeigen auffällig hohe Fehlerraten und werden daher in einer eigenen Gruppe zusammengefasst.

Tab. 2: Fehlerstatistik pro Finger und Zeichengruppe

Tippstatistik	Anzahl Zeichen	Fehleranzahl	Fehlerquote in %
Gesamt (Alle Zeichen)	274.676	7.331	2,67
Kleiner Finger	22.541	758	3,36
Ringfinger	44.946	1.370	3,04
Mittelfinger	89.666	2.279	2,54
Zeigefinger	104.333	2.489	2,39
Third-Level Sonderzeichen	787	88	11,31
Sonderzeichen	10.462	521	4,98
Großbuchstaben	15.435	902	5,84
Zahlen	2056	89	4,33
Kleinbuchstaben	245.945	5.731	2,33

3 EPT – Ergonomic Password Tool

Zur Generierung der ergonomischen Passwörter haben wir die Anforderungen zur Ergonomie in einer Software, dem EPT, umgesetzt. EPT ist ein Kommandozeilen-Programm unter Windows. Der Screenshot des Programms in Abbildung 3 zeigt ein vom EPT generiertes Passwort der Länge zwölf. Neben dem Passwort wird der Sicherheitswert ausgegeben, außerdem der Ergonomiewert. Der Sicherheitswert bestimmt die Güte eines Passwortes nach Sicherheitsrichtlinien des BSI (vgl. [BSI]). Diese ist nur die Standardvorgabe und ist editierbar. Der Ergonomiewert

wird durch die Betrachtung der ergonomischen Anforderungen (vgl. Tabelle 2) hergeleitet. Beide Werte liegen auf einer Skala von 0 bis 100, wobei 100 den bestmöglichen Wert darstellt.

```
C:\EPT>EPTv1.0.1.exe -g 12

Passwort: 5ow73k§HqhSm
Sicherheitswert: 100
Ergonomiewert: 75
```

Abb. 3: Ergonomic Password Tool – Ausgabe eines generierten Passwortes

Das EPT generiert basierend auf dem Ablaufplan in Abbildung 4 und den in der Abbildung angezeigten Konfigurationsdaten zeichenweise Passwörter, die den Anforderungen in Tabelle 1 genügen. Die Auswahl des Pfades wird mithilfe von Pseudozufallszahlen ermittelt.

Wie in Abbildung 4 zu sehen ist, gibt es verschiedene Werte, von denen das nächste Zeichen abhängig ist. Diese Werte wurden aus Dvoraks Thesen und der Statistik (vgl. Tabelle 2) abgeschätzt. Hierbei handelt es sich um Standardwerte, welche Benutzer spezifisch anpassen können. Die Konfigurationsdaten stellen Wahrscheinlichkeiten für die jeweiligen Zeichen des Passwortes dar. Die Wahrscheinlichkeiten an den Entscheidungen sagen aus, dass sich mit dieser Wahrscheinlichkeit für „ja“ entschieden wird. Zudem wird in den Standardeinstellungen davon ausgegangen, dass es sich bei dem Benutzer um einen Rechtshänder handelt. Zum Generieren des ersten Zeichens im Passwort wird davon ausgegangen, dass ein vorheriges Zeichen auf der schwachen Hand getippt wurde. In dieser Version des EPT ist es noch nicht möglich, dass Leerzeichen als Zeichen im Passwort vorkommen können. Bei der Generierung werden folgende 96 Zeichen berücksichtigt:

{ a-z; A-Z; 0-9; ^; °; !; ”; §; $; %; &; /; (;); =; ?; +; *; ’; #; ∼; Komma; Semikolon; Punkt; Doppelpunkt; -; _; @; ?; |; {; [;]; }; \; <; > }

4 Praxistest

Um zu testen, ob durch ergonomisch generierte Passwörter eine Verbesserung der Anschlagraten und eine Reduktion der Fehlerraten erreicht werden kann, eignet sich ein Praxistest. Der Ablauf und die Ergebnisse sind in den folgenden Unterkapiteln beschrieben.

4.1 Datenerhebung

In einem Praxistest wurden das EPT an 18 Probanden erprobt, die in zwei Gruppen eingeteilt wurden. Dazu wurden den Probanden in zwei Runden Passwörter gleicher Länge vorgelegt, die einzugeben waren. Die erste Gruppe G_1 startete mit von KeePass generierten Passwörtern. Es folgten Passwörter, die unter ergonomischen Gesichtspunkten mittels EPT generiert wurden. Den Probanden wurde bei Durchführung des Tests vorenthalten, ob Sie zuerst KeePass- oder EPT-Passwörter eingeben. Die Generierung der EPT-Passwörter erfolgte nach den Vorgaben aus Abbildung 4. Die zweite Gruppe G_2 startete genau umgekehrt. Die Tabelle 3 zeigt die Verbesserung (Verb. in %) der Anschläge (A/min) und die Verringerung der Fehlerraten (jeweils in Prozent) der EPT-Passwörter im Vergleich zu den KeePass-Passwörtern.

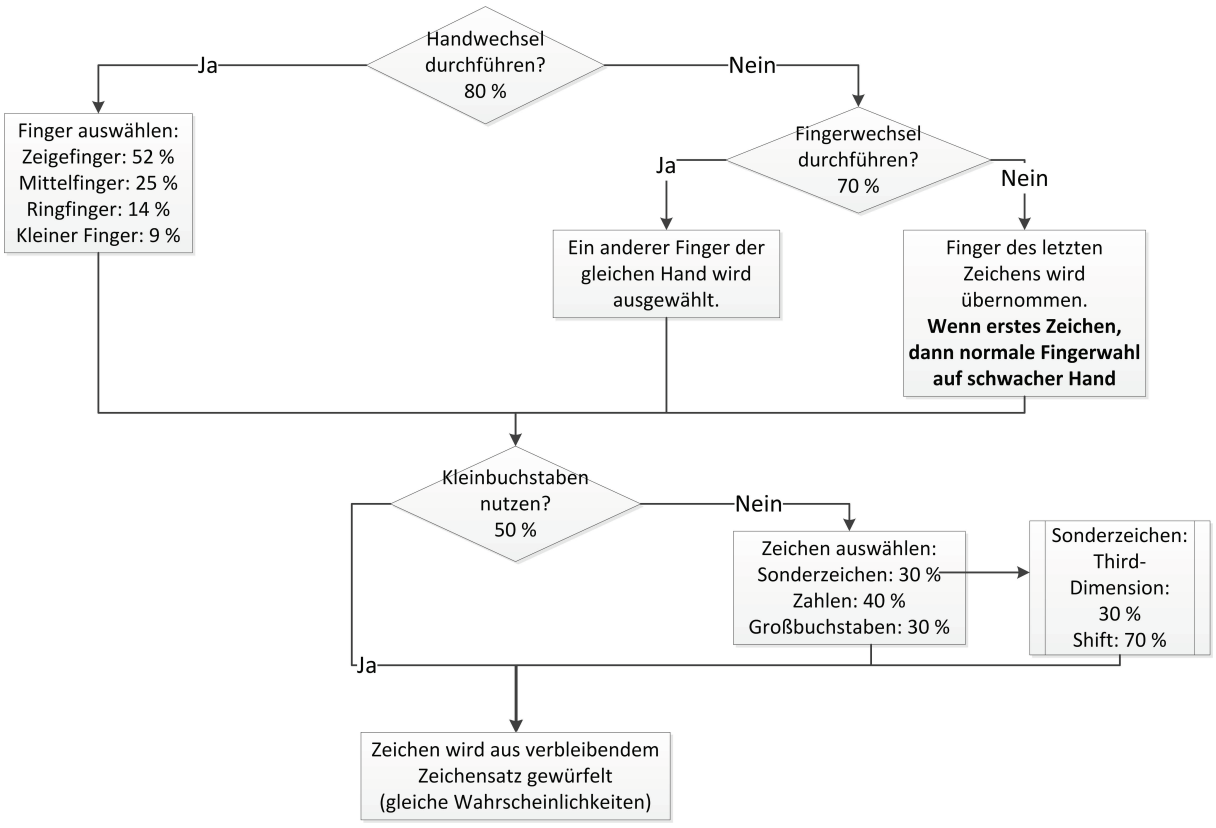

Abb. 4: EPT – Programmablauf zur Generierung eines Passwortzeichens

4.2 Auswertung des Praxistests mittels t-Test

Die Auswertung der Testergebnisse erfolgte mithilfe eines Zweistichproben-t-Tests für abhängige Stichproben nach [HaEK98]. Dieser Test wird verwandt, da wir aufgrund des zentralen Grenzwertsatzes von einer Normalverteilung der Messwerte ausgehen können. Wir wenden den t-Test für die Tippgeschwindigkeit und die Fehlerrate an.

Für die Anschläge pro Minute wurden folgende Thesen aufgestellt:

H_0 : EPT-Passwörter zeigen keine Verbesserung bezüglich der Anschläge pro Minute im Vergleich zu KeePass-Passwörtern:

$$\mu_{KeePass} - \mu_{EPT} \geq 0$$

H_1 : EPT-Passwörter zeigen eine Verbesserung bezüglich der Anschläge pro Minute im Vergleich zu KeePass-Passwörtern:

$$\mu_{KeePass} - \mu_{EPT} < 0$$

Zur Berechnung wurde aus den in Tabelle 3 angegebenen Mittelwerten der Anschläge pro Minute die Differenz gebildet und die Stichprobenstandardabweichung s_d errechnet. Damit ergeben sich die Werte: Größe der Stichprobe: $n = 18$; arithmetischer Mittelwert der Differenzen: $\bar{d} = -12,27$; Stichprobenstandardabweichung: $s_d = 10,52$.

Bei Berechnung der Teststatistik mit der Formel

$$t = \sqrt{n}\frac{\bar{d}}{s_d}$$

Tab. 3: Ergebnisse des Benutzertest

Proband	A/min KeePass	A/min EPT	Differenz der A/min	Verb. in %	Fehler KeePass	Fehler EPT	Differenz der Fehler	Verb. in %
$G_1 - 1$	75	97	-22	29,33	24	6	18	75,00
$G_1 - 2$	49	68	-19	38,78	18	11	7	38,89
$G_1 - 3$	63	76	-13	20,63	13	5	8	61,53
$G_1 - 4$	58	76	-18	31,03	28	11	17	60,71
$G_1 - 5$	50	95	-45	90,00	14	1	13	92,86
$G_1 - 6$	63	83	-20	31,74	25	13	12	48,00
$G_1 - 7$	92	96	-4	4,34	9	5	4	44,44
$G_1 - 8$	46	58	-12	26,08	46	10	36	78,26
$G_1 - 9$	70	74	-4	5,71	24	16	8	33,33
$G_2 - 1$	62	70	-8	12,90	15	6	9	60,00
$G_2 - 2$	52	61	-9	17,31	12	6	6	50,00
$G_2 - 3$	56	61	-5	8,93	16	16	0	0,00
$G_2 - 4$	67	68	-1	1,50	9	3	6	66,67
$G_2 - 5$	110	125	-15	13,63	21	7	14	66,67
$G_2 - 6$	59	68	-9	15,25	7	6	1	14,28
$G_2 - 7$	68	69	-1	1,47	15	13	2	13,33
$G_2 - 8$	64	67	-3	4,69	5	2	3	60,00
$G_2 - 9$	80	93	-13	16,25	9	9	0	0,00
Mittelwert	65,77	78,06	-12,27	18,65	17,22	8,11	9,11	52,90

erhalten wir für oben genannte Werte $t = -4,95$.

Wir testen zum Niveau $\alpha = 0,001$. Damit ergibt sich

$$t_{\alpha;n-1} = -t_{1-\alpha;n-1} = -t_{0,999;17} = -3,646 \Rightarrow t < t_{0,001;17}.$$

Da $t = -4,95 < -3,646 = t_{\alpha,n-1}$ treffen wir die Entscheidung H_1 mit $99,9\%$. Daraus folgt, dass durch die Verwendung von EPT-Passwörtern wahrscheinlich höhere Anschlagraten zu erzielen sind.

Auch die Gesamtfehleranzahl der getesteten Passwörter wurde dem Test unterzogen. Hier lauten die Thesen:

H_0 : EPT-Passwörter zeigen keine Verringerung der Fehleranzahl im Vergleich zu KeePass-Passwörtern.

$$\mu_{KeePass} - \mu_{EPT} \leq 0$$

H_1 : EPT-Passwörter zeigen eine Verringerung der Fehleranzahl im Vergleich zu KeePass-Passwörtern.

$$\mu_{KeePass} - \mu_{EPT} > 0$$

Die Differenz der Mittelwerte der Fehleranzahl aus Tabelle 3 ist $\bar{d} = 9,11$. Daraus folgt die

Stichprobenstandardabweichung $s_d = 8,69$. Die Teststatistik ist dann $t = 4,24$. Bei dem Niveau $\alpha = 0,001$ erhält man das Quantil

$$t_{1-\alpha;n-1} = t_{0,999;17} = 3,646 \Rightarrow t > t_{0,999;17}.$$

Da $t > t_{0,999;17}$ treffen wir die Entscheidung H_1 mit $99,9\%$. Somit ist es durch die Verwendung von EPT-Passwörtern wahrscheinlich, niedrigere Fehleranzahlen zu erzielen.

Anhand der Tabelle 3 ist erkennbar, dass Verbesserungen unabhängig von der Tippgeschwindigkeit zu erzielen sind. Es ist demnach nicht zwingend erforderlich, das Zehnfingersystem schnell zu beherrschen, um von den ergonomischen Passwörtern zu profitieren.

5 Diskussion

Wie in Abbildung 1 zu sehen, sollte ein ideales Passwort den drei Kriterien Sicherheit, Merkbarkeit und Ergonomie genügen. Vor allem mit der Sicherheit von EPT-Passwörtern muss sich kritisch auseinandergesetzt werden. Allerdings spielt auch die Merkbarkeit eine wichtige Rolle bei der Akzeptanz von Passwörtern.

5.1 Sicherheit

Um die Sicherheit ergonomischer Passwörter beurteilen zu können, haben wir praktische und theoretische Ansätze verfolgt. Diese sind in den folgenden Unterkapiteln erklärt.

5.1.1 Angriffe

In einem zwanzigstündigen Testlauf wurde eine Liste von sechs Zeichen langen, EPT-generierten Passwörtern mit dem Passwortcracking-Tool *John the Ripper* [Joh] an mehreren Rechnern abgearbeitet. Während des Testzeitraumes konnte in keinem der ausgeführten Modi (inkrementell, Wörterbuch) ein erfolgreicher Angriff durchgeführt werden. Als Grundlage der Wörterbuchattacke wurden jene Wortlisten verwendet, die auch dem Sicherheitstest des EPT zugrunde liegen. Diese beinhalten unter anderem häufig verwendete Passwörter und Passwortteile.

Die Standard-Einstellungen (vgl. Abbildung 4) des Generators lassen Angriffe über Passwort-Wörterbücher zu, die alle EPT-Passwörter über einem vorgegebenen Wahrscheinlichkeits-Threshold enthalten. So hat das Passwort „$jfjfjfjfjf$“ eine Auftrittswahrscheinlichkeit von $P(jfjfjfjfjf) = 2,51 \cdot 10^{-15}$, wohingegen das sehr unwahrscheinliche Passwort „@|@|@|@|@|“ eine Auftrittswahrscheinlichkeit von $P(@|@|@|@|@|) = 5,89 \cdot 10^{-33}$ hat. Die Werte leiten sich aus den Standardwerten aus dem Ablaufdiagramm in Abbildung 4 her. Im Gegensatz dazu ist die Auftrittswahrscheinlichkeit von gleichverteilten Passwörtern in einem Zeichenraum von 96 Zeichen $P = 1,50 \cdot 10^{-20}$. Diese Werte zeigen klar, dass die Ergonomie und Sicherheit bezogen auf die Auftrittswahrscheinlichkeit eines Passwortes negativ korreliert sind. Eine Erhöhung der Ergonomie geht auf Kosten der Sicherheit und umgekehrt. Ähnliche Beobachtungen gelten zwischen Merkbarkeit und Sicherheit wie das Beispiel der Environ-Passwörter zeigt.

Trotzdem haben ergonomische Passwörter ihre Berechtigung, da in der Praxis oft Wert auf sichere und vom Anwender akzeptierte, also merkbare und ergonomische Passwörter gelegt wird. Einem Wörterbuch-Angriff kann durch die Verlängerung der EPT-Passwörter begegnet werden. Zudem können Benutzer die Standard-Einstellungen an ihre Biometrie anpassen, was

einen Wörterbuchangriff weiter erschwert. Die Verlängerung der EPT-Passwörter von z.B. zehn auf zwölf Zeichen wird durch die um durchschnittlich knapp 20 % schnellere Eingabe der EPT-Passwörter (vgl. Tabelle 3) kompensiert. Zusätzlich schlagen wir eine Blacklist der wahrscheinlichsten ergonomischen Passwörter und eine Mindestlänge von acht Zeichen vor. Dadurch erzielen wir akzeptable Werte für Sicherheit und Ergonomie bei den EPT-Passwörtern.

5.1.2 Entropie

Soll die Stärke von Passwörtern unter mathematischen Aspekten berechnet werden, eignet sich neben anderen Ansätzen wie z.B. von [Cach97] vorgeschlagen die klassische Shannon-Entropie [Shan48] als Maß. Diese lässt sich wie folgt berechnen:

$$H_1 = -\sum_{i=1}^{N}(p_i \cdot log_2(p_i)) \tag{1}$$

mit $N =$ Anzahl der Passwörter und $p_i =$ Wahrscheinlichkeit des Passwortes i.

Hierzu betrachten wir zur Veranschaulichung die Auftrittswahrscheinlichkeiten aller Passwörter mit der Länge vier über dem Zeichenraum von 96 Zeichen. Die maximale Entropie wird erreicht, wenn diese Passwörter dieselbe Auftrittswahrscheinlichkeit besitzen. Anhand dieses Wertes können wir die Stärke von ergonomischen Passwörtern beurteilen.

Die Entropie von vierstelligen gleichverteilten Passwörtern ist $H_{Max_4} \approx 26$. Vierstellige ergonomische Passwörter haben einen Entropie-Wert von $H_{EPT_4} = 19,66$. Betrachten wir auch hier eine Verlängerung der ergonomischen Passwörter um etwa 20%, so erhalten wir einen Entropie-Wert von $H_{EPT_5} = 23,3$. Damit haben wir fast die Stärke von gleichverteilten Passwörtern erreicht. Auch unter den Gesichtspunkten der Shannon-Entropie erzielen wir also mit ergonomischen Passwörtern akzeptable Werte für die Sicherheit.

5.2 Merkbarkeit von EPT-Passwörtern

Passwörter, die mit EPT generiert werden, genügen den Ansprüchen der Sicherheit und der Ergonomie. Weiterhin ist die Merkbarkeit ein wichtiger Faktor für die Wahl eines Passwortes. Das EPT enthält einen Algorithmus zum Generieren merkbarer Passwörter. Dieser funktioniert nach der Beschreibung in [Ande08] zum Erstellen merkbarer Passwörter. Als Ausgabe bekommt der Benutzer nicht nur das merkbare Passwort angezeigt, sondern auch einen Sicherheits- und Ergonomiewert. Der Benutzer kann mit diesen Angaben selbst wählen, ob das erzeugte Passwort seinen Ansprüchen genügt. Dadurch ist im EPT eine teilautomatisierte Lösung zum Erstellen eines „idealen“ Passwortes nach Abbildung 1 gegeben.

6 Fazit und Ausblick

In dieser Ausarbeitung haben wir Anforderungen an die Ergonomie von Passwörtern abgeleitet (Tabelle 1). Diese wurden im EPT umgesetzt. Im nächsten Schritt testeten wir die Passwörter im Vergleich zu rein sicherheitsorientieren Passwörtern. Die dargestellten Ergebnisse des Praxistests zeigen deutlich, dass es möglich ist, Passwörter so zu gestalten, dass sie vom Anwender schneller und mit geringerer Fehlerrate zu tippen sind. Dies ist auch der Fall, wenn das Zehnfingersystem nicht besonders gut beherrscht wird. Denn auch Probanden mit einer geringen Anschlagrate konnten sich bei den vom EPT generierten Passwörtern in der Anschlagra-

te verbessern und reduzierten ihre Fehleranzahl. Die Anschlagrate steigerte sich um durchschnittlich 18,65 %, die Fehlerrate wurde um durchschnittlich 52 % reduziert. Als problematisch stellt sich die negative Korrelation von Sicherheit und Ergonomie dar, die sich durch eine Verlängerung der Passwortlänge, die Verwendung einer Blacklist und die Anpassung der Standard-Einstellungen kompensieren lassen.

Als zukünftige Arbeiten zur Ergonomie von Passwörtern bieten sich an:

- Ausweitung der Untersuchungen auf englische und Smartphone-Tastaturen
- Berücksichtigung von Passwörtern, die auf QWERTZ-Tastaturen und Smartphones eingegeben werden müssen
- Ausweitung der Untersuchen auf andere Schreibsysteme, wie das Tippen mit zwei Fingern
- Untersuchung der Ergonomie bei in der Praxis eingesetzten Passwörtern (vgl. [Roc])
- Integration des EPT in bestehende Passwortgeneratoren
- Erweiterung und detailliertere Prüfung der Anforderungen durch eine gezielte Betrachtung von Tippfehlern für Buchstabentupel, -tripel und ganze Wörter

Mit den drei oberen Punkten beschäftigt sich [Herr12].

Literatur

[Ande08] R. Anderson: Security Engineering, Second Edition. Wiley (2008).

[BSI] Bundesamt für Informationssicherheit. Abgerufen am: 10.12.2011, https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Passwoerter/passwoerter_node.html.

[Cach97] C. Cachin: Entropy Measures and Unconditional Security in Cryptography. Dissertation, Swiss Federal Institute of Technology Zürich (1997).

[Cas] CASED - Online Passwort Testzentrum. Abgerufen am: 25.01.2012, http://passwortstudie.cased.de/testing/publications/.

[Dat] Datenschutzbeauftragter Katon Zürich - Passwort-Check. Abgerufen am: 20.04.2012, https://passwortcheck.datenschutz.ch/doc/process.de.php.

[Dic] The Diceware Passphrase Homepage. Abgerufen am: 17.04.2012, http://www.diceware.com.

[DIN] DIN 2137 - Tastaturen für die Daten- und Texteingabe - Teil 1: Deutsche Tastaturbelegung.

[HaEK98] J. Hartung, B. Elpelt, K.-H. Klösener: Statistik - Lehr- und Handbuch der angewandten Statistik. Oldenbourg Wissenschaftsverlag, 11. Aufl. (1998).

[Herr12] B. Herres: Reduktion von Fehlerraten mithilfe ergonomisch sicherer Passwörter - Erweiterung des Ergonomic Password Tools für Smartphones. Fachhochschule Trier (2012).

[HeWe12] B. Herres, D. Weich: Reduktion von Fehlerraten mithilfe ergonomisch sicherer Passwörter. Fachhochschule Trier (2012).

[Joh] John the Ripper password cracker. Abgerufen am: 16.04.2012, http://www.openwall.com/john/.

[JoMo88] B. Joyce, R. A. Moxley: August Dvorak (1894-1975): Early Expressions of Applied Behavior Analysis and Precision Teaching. In: *The Behavior Analyst* (1988), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2741848/pdf/behavan00058-0036.pdf.

[Kee] KeePass 2011. Abgerufen am: 29.12.2011, http://www.keepass.info.

[NEO] Neo-Tastaturlayout. Abgerufen am: 29.12.2011, http://neo-layout.org/.

[Roc] RockYou Passwortliste. Abgerufen am: 28.06.2012, http://www.skullsecurity.org/wiki/index.php/Passwords.

[Rohm82] W. Rohmert: Forschungsbericht ergonomische Schreibmaschinentastatur. In: *Bundesministerium für Forschung und Technologie: Forschungsbericht / DV / 82,1-; 82,3* (1982), 116–136, http://forschung.goebel-consult.de/de-ergo/rohmert/Rohmert.html.

[Shan48] C. E. Shannon: A Mathematical Theory of Communication. In: *The Bell System Technical Journal* (1948).

[Stam05] M. Stamp: Information Security. Wiley (2005).

[TIP] Tipp10 - 10-Finger-Schreibtrainer. Abgerufen am: 16.04.2012, http://www.tipp10.com/de/.