Otto-von-Guericke Universität Magdeburg

Fakultät für Informatik
Institut für Technische und Betriebliche Informationssysteme

Bachelorarbeit

Fusion grafischer und textueller Passwörter

Autor:

Melanie Wetzel

18.10.2010

Betreuer:
Prof. Dr.-Ing. Jana Dittmann
Fakultät für Informatik
Otto-von-Guericke Universität
Universitätsplatz 2
39106 Magdeburg

Stefan Kiltz
Fakultät für Informatik
Otto-von-Guericke Universität
Universitätsplatz 2
39106 Magdeburg

Außenbetreuer:
Pascal Held
Sirenen
bewusste Sicherheit
Alter Postweg 80
38518 Gifhorn

Steven Schwenke
Sirenen
bewusste Sicherheit
Alter Postweg 80
38518 Gifhorn

1 Abstract

Grafische Passwortsysteme, wie zum Beispiel PassPoints [5] haben in den vergangenen Jahren immer mehr Aufmerksamkeit erregt. Eine Art Erweiterung dieser grafischen Passwortsysteme um den textuellen Bestandteil herkömmlicher Passwortsysteme stellt bereits das Programm TwoSteps [3] dar. Im Gegensatz zu diesem, in dem zuerst die textuelle und anschließend erst die grafische Passworteingabe erfolgt, bietet der hier beschriebene Ansatz eine neue Möglichkeit die Vorteile beider Systeme miteinander zu vereinen. Für diese Arbeit wurde ein Programm[1] entwickelt, welches es ermöglicht ein Passwort so zu wählen, dass sowohl lexikografische Zeichen als auch Klickpunkte in einem Bild an jede Position des Passwortes geschrieben werden können. Diese Kombination der grafischen und textuellen Passwortsysteme erhöht die Sicherheit vor Angriffen und bietet eine bessere Nutzerfreundlichkeit als reine textuelle Passwortsysteme. Da eine Kombination zweier Systeme nicht immer nur die Vorteile beider mit einander vereint, ergeben sich aus dieser Fusion auch neue Probleme und Risiken, wie zum Beispiel die Nutzung des textuellen Passwortanteils nur als Beschreibung der Klickpunkte.

[1] http://visualpwd.bewusste-sicherheit.de/login.php

Inhaltsverzeichnis

2 Einleitung

Den meisten Menschen fällt es schwer sich alphanumerische Passwörter zu merken, was auch daran liegt, das ein durchschnittlicher Web-User sich Passwörter auf 25 unterschiedlichen Web-Seiten merken muss. [12] Dies führt zu einer Menge unsicherer Strategien, wie zum Beispiel Passwörter aufschreiben, dasselbe Passwort mehrfach verwenden, wenige Varianten eines einzigen Passworts verwenden oder sich das Passwort neu zuschicken lassen. [4] Textuelle Passwörter sind entweder leicht zu merken und unsicher oder schwer zu merken und sicher. Bilder hingegen haben den Vorteil, dass sie sich leichter und länger merken lassen. [1, 11] Die bessere Merkbarkeit wird durch den picture superiority effect in verschiedenen psychologischen Studien vorrausgesagt. [14] Durch diesen Effekt haben Menschen einen enormen, fast unbegrenzten Speicherplatz für Bilder, welche sie sich viel besser und auch viel länger merken können als Worte. Ein Grund für den superiority effect könnte der Fakt sein, dass Menschen Bilder zwei Mal auf verschiedene Arten in ihrem Gedächtnis abspeichern, zum einen als visuelle Konfiguration und zum anderen als lexikografische Beschreibung. Das heißt, wenn man ein Bild eines roten Balles gezeigt bekommt, merkt man sich zum einen wie dieser aussieht und zum anderen das Wort „Ball“. Ein anderer Grund könnte sein, das die Bilder umfangreicher gespeichert werden und es mehr mentale Verbindungen gibt, die zum Wiederauffinden genutzt werden können. [1] Für das Beispiel mit dem Ball bedeutet das, dass man beim Sehen eines anderen Gegenstandes in der Farbe rot ebenfalls an diesen roten Ball denkt, dies geschieht meistens im Unterbewusstsein. Diese Vorteile allein reichen allerdings nicht aus, um reine grafische Passwortsysteme zu verwenden, denn sie bieten keine ausreichende Sicherheit. Da die meisten Anwender die Klicks ihres Passwortes auf einer Linie oder nach einem anderen Muster anordnen [7,9], ist ein möglicher Angreifer, der diese Muster leicht rekonstruieren kann, auch in der Lage das Passwort für seine Zwecke zu missbrauchen. Bei einer Authentifizierung nur mit Hilfe der Maus als einziges Eingabegerät steigt das Risiko eines Shoulder-Surfing-Angriffes [8]. Eine Fusion der textuellen und der grafisches Passworteingabe verbindet die Vorteile beider Systeme.

3 Stand der Technik

Bilder lassen sich auf verschiedene Weise zur Unterstützung der Authentifizierung nutzen, hierbei werden drei wesentliche Gruppen unterschieden: Searchmetric, Drawmetric und Locimetric Systems. [1]

3.1 Searchmetric System

In Searchmetric Systemen wird der Nutzer bei der Registrierung dazu aufgefordert eine Anzahl von Bildern auszuwählen, so dass daraus der Authentifizierungsschlüssel erstellt wird. Bei einer darauffolgenden Authentifizierung wird dem Nutzer eine gewisse Anzahl von Bildern vorgelegt, welche den Authentifizierungsschlüssel und eine bestimmte Anzahl von falschen Bildern beinhalten. [1] Systeme, die auf dem Searchmetric Modell basieren, sind heute bereits auf dem Markt erhältlich. Beispiele hierfür sind Pointsec[1], und Lockscreen siehe Abbildung 3.1. Beide wurden für die Anwendung auf einem PDA entwickelt und verwenden Icons zur Authentifizierung.

Abbildung 3.1: Searchmetric Modelle am Beispiel Pointsec (links) und Lockscreen (rechts).[1]

Ein weiteres Searchmetric System ist $Passfaces^{TM}$[2]. Passfaces ist vermutlich das am meist genutzte grafische Passwortsystem. [1] In Abbildung 3.2 ist auf der linken Seite

[1] http://www.pointsec.com/core/default.asp
[2] http://www.realuser.com/

ein Einloggscreen dargestellt und auf der rechten Seite der Authentifizierungsprozess. Zur Authentifizierung wird hierbei ein 3x3 Gitter mit Gesichtern dargestellt. Zur erfolgreichen Authentifizierung ist es erforderlich, dass der Nutzer das richtige Gesicht aus jedem Gitter auswählt. Hierbei kann die Länge der Sequenz variiert werden, je nachdem wofür die Applikation verwendet wird. Passfaces sind für verschiedene Dinge einsetzbar, beispielsweise auf dem traditionellen Desktop, auf PDAs und Mobiltelefonen. [4] Anstelle der Bilder von Gesichtern können auch natürliche Fotos oder Kunstbilder verwendet werden. Eine Studie von Dhamija und Perring [15] ergab, dass die Fehlerrate bei der Verwendung von Kunstbildern nach einer Woche 10% betrug und bei Fotografien nur 5%.

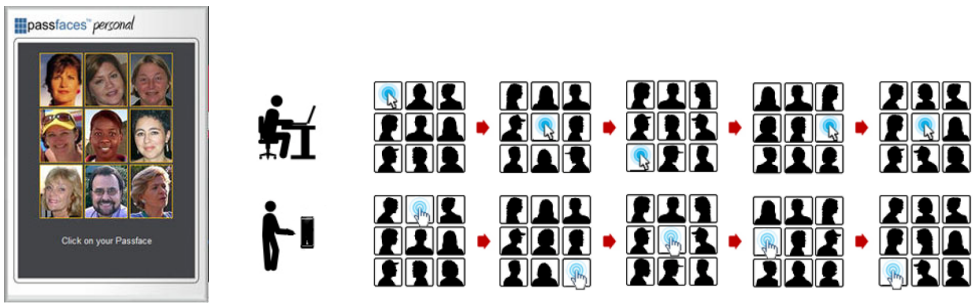

Abbildung 3.2: Searchmetric Modell am Beispiel Passfaces. Links: Beispiel für einen Einloggscreen. [21] Rechts: Darstellung des Authentifizierungsprozesses. [4]

3.2 Drawmetric System

In Drawmetric Systemen wird vom Nutzer verlangt, ein einfaches Bild zu zeichnen, dieses stellt dann das Passwort dar. Beispiele für solche frei vom Nutzer gezeichneten grafischen Passwörter sind das Draw-a-Secret Schema (DAS)[16,2], Pass-Go [6] und Schemen, in denen durch drag and drop einzelner Basisformen das Nutzerpasswort zusammengesetzt wird.

Beim DAS Schema werden Linien auf eine Fläche gezeichnet, deren Hintergrund ein Gitter zeigt. Ein Gitter als Hintergrund zu verwenden, hat zwei Vorteile: zum einen erspart es die Nutzung einer grafischen Datenbank auf dem Server und zum anderen ist ein Raster ein einfaches Objekt, wodurch das DAS Schema auch auf Geräten mit geringerer Auflösung verwendet werden kann. Die aktuelle Zeichnung des Nutzers wird auf dem Display dargestellt, siehe Abbildung 3.3 links. Ein DAS-Passwort kann beliebig lang sein und wird kodiert durch die Sequenz der Gitterzellen, die als zweidimelsionale Koordinatenpaare repräsentiert werden. Das Passwort für das Beispiel in Abbildung 3.3 links wird als (2,2), (3,2), (3,3), (2,3), (2,2), (2,1), (5,5) gespeichert, wobei (5,5) ein spezielles Koordinatenpaar ist, welches symbolisiert, dass hier der Stift abgesetzt wurde.

Das Pass-Go Schema wurde von einem alten chinesischen Spiel namens Go inspiriert und basiert ebenfalls auf einem gitterbasierten Schema. Bei Pass-Go werden die Gitterkreuzungen anstatt der Gitterzellen angeklickt. Da es schwierig ist genau diesen einen

Punkt anzuklicken, gibt es so genannte Sensitive Areas, angeordnet um die Gitterkreuzungen. Das in Abbildung 3.3 rechts dargestellte Passwort wird als (4,8), (4,7), (4,6), (0,0), (4,6), (5,6), (5,5), (6,6), (0,0), (7,7), (7,6), (7,5), (0,0) gespeichert, wobei hier das Koordinatenpaar (0,0) das Stiftabsetzen darstellt.

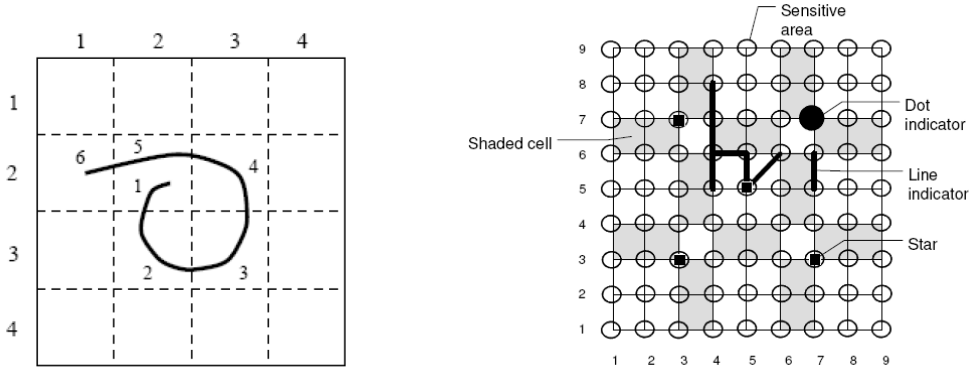

Abbildung 3.3: Drawmetric Systeme, links: DAS und rechts: Pass-Go [6]

3.3 Locimetric System

Bei locimetrischen Systemen wird vom Nutzer das Anklicken der Punkte in einem Bild zur Registrierung und das Merken dieser in der richtigen Reihenfolge gefordert, um sie beim erneuten Einloggen korrekt wieder zu geben.

3.3.1 PassPoint

Eines der grundlegenden locimetrischen Systemen ist PassPoints (PP). PassPoints ist ein Klickbasiertes grafisches Passwortsystem, bei dem das Passwort aus einer Sequenz von fünf Klicks auf einem Bild besteht, siehe Abbildung 3.4. [5] Beim Einloggen muss der Nutzer jeden Klick innerhalb einer vom System definierten Toleranz Region setzen. Das Bild wirkt dabei als Hinweisgeber, um dem Nutzer zu helfen sich an sein Passwort zu erinnern.

Einige Studien [17,18] ergaben, dass bestimmte Bereiche eines Bildes häufiger vom Nutzer geklickt werden als andere, diese Bereiche nennt man Hotspots, dargstellt in Abbildung 3.4. Ein Angreifer ist in der Lage diese Hotspots zu erraten oder mit Hilfe von Bildbearbeitungstechniken zu ermitteln und daraus ein Wörterbuch von häufig geklickten Punkten zu bilden. [7] Des Weiteren hat sich in wissenschaftlichen Untersuchungen gezeigt, dass die Klickpunkte meistens auf einer Linie liegen oder einem anderen Muster, wie z.B. einem Buchstaben folgen, siehe Abbildung 3.5.

Abbildung 3.4: Links: Ein PassPoints Passwort bestehend aus fünf geordneten Klicks (die Zahlen werden in der Umsetzung nicht angezeigt).[5] Rechts: Hotspots. [1]

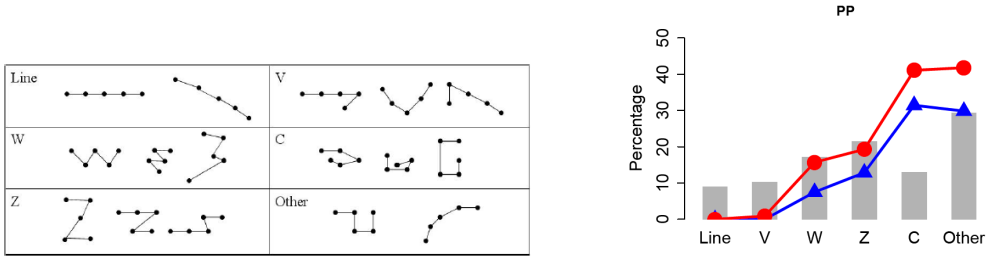

Abbildung 3.5: Links: Beispiele für Klickpunkt Muster. Rechts: Das Diagramm zeigt, die Prozente der Passwörter, die unter die jeweilige Kategorie fallen. Die rote und blaue Linie zeigen den Maximum- und Minimummittelwert. [7]

3.3.2 Cued Click-Points

PassPoints schien ein nutzbares System zu sein und erfuhr eine Art Weiterentwicklung zu CCP (Cued Click-Points). CCP [19] wurde als alternatives Klick-basiertes grafisches Passwort Schema entwickelt, bei dem der Nutzer einen Punkt je Bild auswählt für fünf Bilder, siehe Abbildung 3.6. Das Interface zeigt zu jedem Zeitpunkt ausschließlich ein Bild. Der Bildwechsel erfolgt sobald der Nutzer einen Klickpunkt ausgewählt hat. Welches Bild als nächstes erscheint, hängt vom zuvor geklickten Punkt ab. Dieses entwickelte System hat Vorteile, was die Sicherheit als auch die Nutzerfreundlichkeit betrifft. Der Benutzer muss sich nur noch einen Klickpunkt pro Bild merken und bei einem Fehlklick, wird dies sofort anhand des falsch vorliegenden Bildes bemerkt. Dieses direkte Feedback ist für den Nutzer sehr hilfreich, für einen Angreifer allerdings nicht, da dieser die Reihenfolge der Bilder nicht kennt.[7] Eine Laborstudie [19] hat gezeigt, das CCP die gleiche Benutzerfreundlichkeit wie PassPoints aufweist, zusätzlich aber den Vorteil weniger häufig auftretender Hotspots.

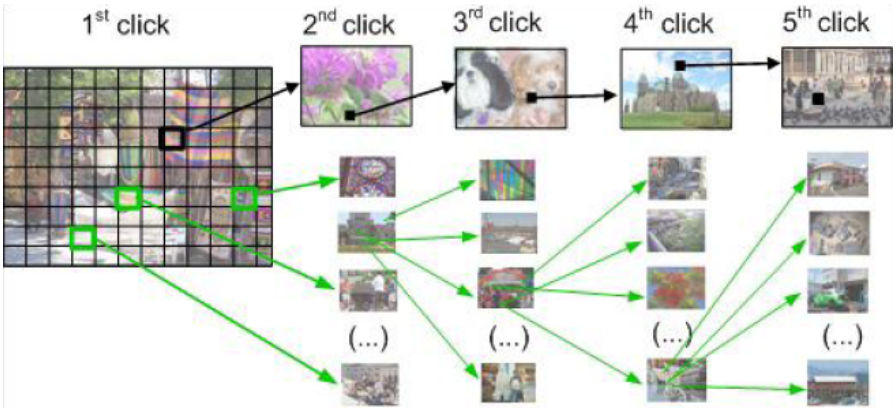

Abbildung 3.6: Bei CCP wählt der Nutzer je Bild einen Klickpoint aus. Welches Bild als nächstes erscheint, hängt vom zuvor geklickten Punkt ab. [7]

3.3.3 Persuative Cued Click-Points

Um den Aspekt der Hotspots zu vermeiden, wurde der persuative Cued Click-Points (PCCP) [20] Ansatz entwickelt. Genau wie bei CCP besteht ein Passwort aus fünf Klickpunkten, einem auf jedem der fünf Bilder. Während der Registrierung wird ein Großteil des Bildes bis auf ein kleines Sichtfenster abgedunkelt. Dieses Sichtfenster ist zufällig gewählt und der Nutzer wird dazu aufgefordert seinen Klickpunkt innerhalb des Rechteckes zu positionieren, siehe Abbildung 3.7.

Sollte ein Nutzer innerhalb dieses Sichtfensters keinen Punkt setzen wollen, kann er den Shuffle Knopf betätigen, um ein neues zufälliges Sichtfenster erzeugen zu lassen. Mit Hilfe dieses zufällig vorgegebenen Sichtfensters wird der Nutzer dazu geleitet ein Passwort zu kreieren, welches seltener Hotspots beinhaltet. Natürlich ist es möglich so lange die Shuffle-Funktion zu verwenden bis das Sichtfenster an der gewünschten Position angezeigt wird, dies würde allerdings erheblich mehr Zeit beanspruchen. Da die meisten Nutzer gewillt sind, den Weg des geringsten Widerstandes zu gehen, werden sie eines der ersten Sichtfenster zur Auswahl des Klickpunktes verwenden. Als Ergebnis können durch PCCP stärkere Passwörter erstellt werden. [7]

3.4 TwoSteps

In TwoSteps wird eine Authentifikationsmethode zur Stärkung der textuellen Passwörter beschrieben, in dem diese mit grafischen Passwörtern kombiniert werden. [3] Da textuelle Passwörter einfach in der Anwendung und im Gebrauch sind, werden sie sicher beliebt bleiben. Da es aber Angriffsmöglichkeiten wie Brute-Force und Phishing Attacken gibt, sind textuelle Passwörter allein nicht sicher genug. Bei TwoSteps wird zuerst ähnlich anderer Authentifizierungssystemen auch nach dem Benutzernamen und dem Textpasswort gefragt. Unabhängig davon, ob diese Eingabe korrekt war, wird dem Nutzer anschließend ein Portfolio angezeigt. Aus diesem Portfolio muss der Nutzer alle die Bilder anklicken,

Abbildung 3.7: Die Benutzeroberfläche von PCCP. Der Nutzer wird dazu aufgefordert seinen Klickpunkt innerhalb des heller dargestellten Sichtfensters zu setzen. Mittels des Shuffle Knopfes wird das Sichtfenster an einer neuen zufälligen Position erzeugt. [7]

die er zuvor im Registrierungsschritt ausgewählt hat. Sollte das grafische Passwort inkorrekt ausgewählt werden, wird der Zugang verwehrt, trotz dessen das textuelle Passwort stimmte. Sollte das textuelle Passwort falsch eingegeben worden sein, enthält das Portfolio nicht die korrekten Bilder, die der Nutzer zur Authentifikation benötigt. Wenn der Nutzer dies feststellt, kann er mit Hilfe eines Go-Back Knopfes zurück zu Schritt eins gehen, um dort das Textpasswort zu korrigieren. TwoSteps liefert folgende Vorteile im Vergleich zu herkömmlichen textuellen Passwörtern: 1. die Einloggerfahrung des Nutzers bleibt weitestgehend erhalten; 2. ein gestohlenes Textpasswort allein gefährdet nicht den Account; 3. der Nutzer wird durch das Nichtsehen des grafischen Passwortes direkt über ein inkorrektes Passwort alarmiert; und 4. es kann mit Hilfe von Software allein umgesetzt werden. [3]

4 Konzept der Fusion

Das Wort Fusion stammt aus dem lateinischen und bedeutet so viel wie Schmelzen. Das Prinzip der Fusion findet bereits in einigen biometrischen Authentifizierungssystemen Anwendung.[10, 13] Das im Rahmen dieser Bachelorarbeit entwickelte Login-System vereint die Möglichkeit der grafischen mit der textuellen Passworteingabe. Im Gegensatz zu TwoSteps, bei dem zuerst nach der textuellen Passworteingabe gefragt und anschließend erst der grafische Teil abgehandelt wird, finden die beiden Prozesse in diesem Ansatz gleichzeitig statt. Da keine Mindestangabe für verwendete Zeichen und Klickpunkte vorliegt, ist es prinzipiell möglich, ein reines Textpasswort zu erstellen oder eines, welches nur aus Klickpunkten besteht, anzuwenden. Im Optimalfall sollte die Anzahl der Klickpunkte und der Zeichen jedoch nicht null sein. Ein Passwort könnte beispielsweise wie folgt aussehen: „ab[Klickpunkt 1]17[Klickpunkt 2]xd“ (siehe Abbildung 4.1).

Abbildung 4.1: Bild mit zwei möglichen Klickpunkten.

5 Prototypische Implementierung

Das Programm wurde durch eine JavaScript-Programmierung erstellt und lässt sich über einen Internetbrowser öffnen. Beim Öffnen der Startseite wird dem Nutzer die Wahl zwischen neu registrieren oder authentifizieren gegeben, siehe Abbildung 5.1.

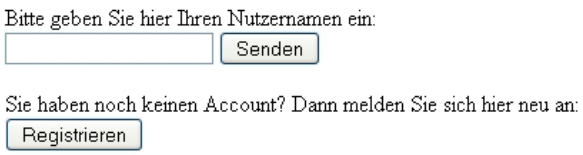

Abbildung 5.1: Screenshot der Startseite.

5.1 Registrierung

Wählt der Nutzer die Registrierung aus, gelangt er zu einem neuen Fenster, in dem er ein Foto [22], darunter drei Eingabefelder und einen Knopf angezeigt bekommt (siehe Abbildung 5.2).

Des Weiteren wird ihm ein Feld mit hundert Koordinaten im Bild zufällig generiert, siehe Quellcode 5.1. Die Punkte bekommen je einen X-Wert im Bereich zwischen null und der Breite des Bildes und einen Y-Wert im Bereich zwischen null und der Höhe des Bildes. Zufällig generiert werden die Werte durch die math.random Funktion. Diese Koordinaten stellen die möglichen Klickbereiche dar, eine mögliche Unterteilung zeigt Abbildung 5.3. Diese Bereiche sind für jeden Nutzer unterschiedlich und werden nicht angezeigt.

```
1 for (var j = 0; j < Zufallsfeld.length; j++)
2 {
3         zfeld[0][j] = Math.floor(Math.random()*Bild.width);
4 }
5 for (var k = 0; k < Zufallsfelf.length; k++)
6 {
7         zfeld[1][k] = Math.floor(Math.random()*Bild.height);
8 }
```

Listing 5.1: Generierung des Zufallsfeldes.

Abbildung 5.2: Screenshot der Registrierungsanzeige.

In die drei Eingabefelder sind vom Nutzer Eintragungen vorzunehmen, in das Feld vor dem User steht, der, vom Nutzer ausgewählte Nutzername und in dem Passwort-Feld sein Passwort. Für dieses Passwort können vom Nutzer sowohl Buchstaben, Zahlen und andere Zeichen, die auf der Tastatur vorhanden sind, als auch Klickpunkte im Bild verwendet werden.

Bei einer textuellen Eingabe werden die Zeichen direkt in das Feld eingetragen und sind für den Nutzer nicht sichtbar, sondern werden nur als Platzhalter angezeigt. Bei der Verwendung von einem Klickpunkt, wird dieser dem Nutzer ebenfalls als Platzhalter im Passwort-Feld dargestellt. Hier wird jedoch nicht die eigentliche Koordinate gespeichert. Bei der Verwendung eines Klickpunktes wird eine Funktion aufgerufen, die den euklidischen Abstand berechnet, die Formel lautet wie folgt: $s = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$, siehe Quellcode 5.2. In der For-Schleife wird der Abstand zwischen Klickpunkt und jedem der hundert Zufallspunkte berechnet. Von dem Punkt des Zufallsfeldes, der dem des Klickpunktes am Nächsten liegt, wird die Position im Zufallsfeld zurück gegeben. Bei beispielsweise einer Länge von fünf Zufallskoordinaten, die lauten: [10,15],[0,4],[12,8],[5,19],[17,7]

Abbildung 5.3: Unterteilung des Bildes in hundert Bereiche. Die roten Punkte stellen die Zufallspunkte dar und die blauen Linien grenzen die Bereiche ab.

und einem Klickpunkt mit den Koordinaten [1,3], wäre die Koordinate [0,4] die zum Klickpunkt nächstgelegene Koordinate und damit würde hier die Position zwei zurück gegeben werden.

```
1 for (i = 0; i < Zufallsfeld.length; i++)
2 {
3         xWertProdukt=((xwert-zfeld[0][i]) * (xwert-zfeld[0][i]));
4         yWertProdukt=((ywert-zfeld[1][i]) * (ywert-zfeld[1][i]));
5         Abstand = Math.sqrt(xWertProdukt+yWertProdukt);
6         if (Abstand < minAbstand)
7         {
8                 minAbstand = Abstand;
9                 minp = i;
10        }
11 }
12 return minp;
```

Listing 5.2: Berechnung der am Nächsten liegenden Zufallskoordinate.

Aber auch diese Position wird nicht in das Passwortfeld geschrieben sondern ein Unicode-Zeichen. Diese Unicode-Zeichen werden zuvor generiert und jedem der hundert Koordinaten des Zufallsfeldes ein eigenes Unicode-Zeichen zugewiesen, siehe Quellcode 5.3. Die Zahl 384 steht für das Unicode-Zeichen 384 und mittels der For-Schleife

werden die Unicode-Zeichen von 384 bis 483 verwendet. Von der Position im Zufallsfeld, die zuvor berechnet wurde, wird nun das Unicode-Zeichen verwendet. Für das angeführte Beispiel heißt das, da die Distanzfunktion die Position zwei zurück gegeben hat, wird das zweite Unicode-Zeichen verwendet. In diesem Fall wäre das Zeichen Nummer 385.

```
1         for (i =0; i < Zufallsfeld.length; i++)
2         {
3                         UnicodeFeld[i] = String.fromCharCode(384+i);
4
5         }
6         var x = UnicodeFeld[position];
7         return x;
```

Listing 5.3: Generierung der Unicode-Zeichen.

Der Grund für das Zufallsfeldverfahren ist, dass die Hashbarkeit der Klickpunkte erleichtert wird. Denn würde man sie direkt hashen, müsste der Nutzer beim Wiederholen des Passwortes die exakte Koordinate erneut treffen, da diese dann in der Datenbank stünde. Durch die Unterteilung des Bildes steht dem Nutzer ein gewisser Bereich zur Verfügung, in dem er seinen Klickpunkt setzen kann und das Passwort korrekt erkannt wird, auch ohne das der exakte Punkt wieder getroffen werden muss.

In das Feld, vor dem „Passwort wiederholen“ steht, muss der Nutzer sein Passwort erneut korrekt eingeben. Wenn die Felder nun vollständig ausgefüllt wurden, klickt der Nutzer den Registrieren-Knopf und bekommt sofort Rückmeldung in Form einer kurzen Nachricht über die erfolgreiche Registrierung oder über den Fehlversuch der Passwortwiederholung. Bei einer erfolgreichen Registrierung werden der Nutzername, das gehashte Passwort und das Feld der hundert Zufallskoordinaten an eine Datenbank gesendet und dort gespeichert.

5.2 Authentifikation

Um sich zu authentifizieren, muss der Nutzer zuerst seinen Nutzernamen eingeben und diesen mit dem Klick auf einen Senden-Knopf bestätigen. Sollte dieser Nutzer nicht in der Datenbank gespeichert sein, wird dem Anwender dies mitgeteilt. Wenn zu dem Nutzernamen bereits ein Account angelegt wurde, werden die Zufallskoordinaten beim senden geladen und der Nutzer kann im nächsten Schritt sein Passwort eingeben (siehe Abbildung 5.4). Mit den Klickpumkten wird bei der Authentifizierung ebenso verfahren wie bei der Registrierung, das heißt auch hier werden die Abstände berechnet und das Unicode-Zeichen in das Passwortfeld geschrieben. Stimmt das Passwort mit dem in der Datenbank gespeicherten überein, bekommt der Nutzer eine Seite angezeigt, auf der „login erfolgreich“ steht oder sollte das Passwort inkorrekt sein, steht dort „Passwort falsch“.

Abbildung 5.4: Screenshot der Loginanzeige.

5.3 Passwort ändern und Account löschen

Diese prototypische Implementierung beschränkt sich auf die Registrierung und die Authentifizierung, da diese beiden Interaktionen genügen, um das Prinzip der Fusion zu zeigen. Das Passwort zu ändern, ist derzeit nicht möglich, ließe sich aber bei Bedarf leicht ergänzen. Die Terminierung eines angelegten Accounts ist nur durch den Administrator möglich, aber auch hier ist eine Erweiterung denkbar.

6 Auswertung

Zu Auswertungszwecken und zur groben Abschätzung der Verhaltensmuster der Nutzer wurde eine kleine nicht repräsentative Umfrage vorgenommen. An dieser Umfrage beteiligten sich 20 Personen, darunter waren überwiegend jüngere aber auch ältere Anwender, siehe Tabelle 6.1.

Zur Durchführung dieser Umfrage wurde ein Link zum Login-System verschickt. Beim erfolgreiche und auch beim fehlerhaften Einloggversuch wird dem Nutzer ein Fragebogen als Download zur Verfügung gestellt. Die Fragen waren wie folgt gestellt:

- Wie viele Klickpunkte haben Sie für Ihr Passwort verwendet?
- Wie viele Zeichen haben Sie für Ihr Passwort verwendet?
- Hatten Sie Probleme beim Registrieren bzw. beim Einloggen? Wenn ja, beschreiben Sie bitte das Problem.
- Wie gefällt Ihnen die Möglichkeit, zusätzlich zur herkömmlichen Tastatureingabe auch Klickpunkte zu verwenden?
- Was gefällt Ihnen an dem hier vorgestellten Passwortsystem, was sollte Ihrer Meinung nach verbessert werden?
- Glauben Sie, dass Sie sich Ihr so eben erstelltes Passwort dank der Klickpunkte besser merken können als ein Passwort, welches nur aus reinem Text besteht?
- Wenn Sie die Wahl hätten, würden Sie das hier vorgestellte Passwortsystem dem der reinen Texteingabe vorziehen? Wenn ja warum bzw. wenn nein, warum nicht?
- Sonstige Anmerkungen:

Dem Großteil der Befragten gefiel das hier vorgestellte Login-System und sie konnten sich vorstellen dieses oder ein ähnliches System auch im Alltag zu verwenden, siehe

Alter	Anzahl
unter 20	1
20 bis 30	13
30 bis 40	4
über 40	2

Tabelle 6.1: Anzahl der unterschiedlichen Testpersonen je Altersgruppe.

Abbildung 6.1. Die Nutzer verwendeten unterschiedlich viele Klickpunkte und Zeichen für ihr Passwort, siehe Abbildung 6.2. jedoch nie mehr als vier Klickpunkte und sieben Zeichen.

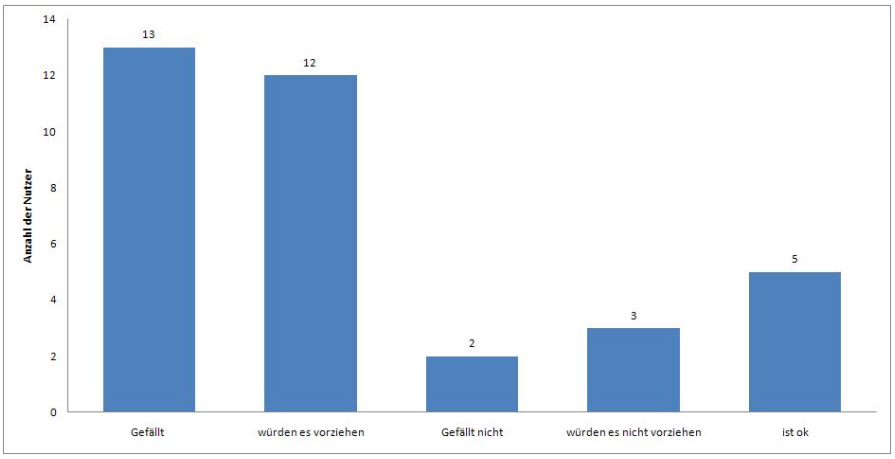

Abbildung 6.1: Die Einstellung der Nutzer zu dem hier vorgestellten Programm.

6.1 Benutzerfreundlichkeit

Das hier vorgestellte Programm ist möglichst einfach strukturiert und zugleich selbsterklärend. Den meisten Nutzern dürfte es nicht schwer fallen ihre Erfahrung vom Registrieren und Anmelden herkömmlicher Login-Systeme auf diese Kombination des grafischen und textuellen Passwortes zu übertragen.

Definiert wird die Benutzerfreundlichkeit in der ISO Norm 9241-11 durch die Kriterien Effektivität, Effizienz und Zufriedenheit.

Die Effektivität, ist die Genauigkeit und Vollständigkeit, mit der Benutzer ein bestimmtes Ziel erreichen [23]. Die Umfrage hat gezeigt, das einige Nutzer Probleme hatten ihren genauen Klickpunkt beim Wiederholen des Passwortes beziehungsweise beim Einloggen zu treffen. Dies liegt an der Unterteilung des Bildes in hundert für jeden Nutzer individuellen Bereiche. Diese Bereiche beim Registrieren anzuzeigen, würde dem Nutzer die Wahl der Punkte erheblich vereinfachen. Trotz dieser anfänglichen Schwierigkeiten waren zu guter Letzt doch alle Nutzer in der Lage sich zu registrieren und anschließend erfolgreich einzuloggen.

Die Effizienz ist der im Verhältnis zur Genauigkeit und Vollständigkeit eingesetzte Aufwand, mit dem Benutzer ein bestimmtes Ziel erreichen [23]. Bei reinen textuellen Passwortsystemen ist der Nutzer durch Verwendung der Tab- und der Enter-Taste in der Lage sich nur mit Hilfe der Tastatur einzuloggen und muss nicht zwischen Tastatur und Maus wechseln. Bei Passwortsystemen, die nur grafische Passwörter verwenden, benötigt der Nutzer lediglich zur Namenseingabe die Tastatur und kann anschließend für den Rest des Logins die Maus verwenden. Also verlangen weder die textuelle noch die

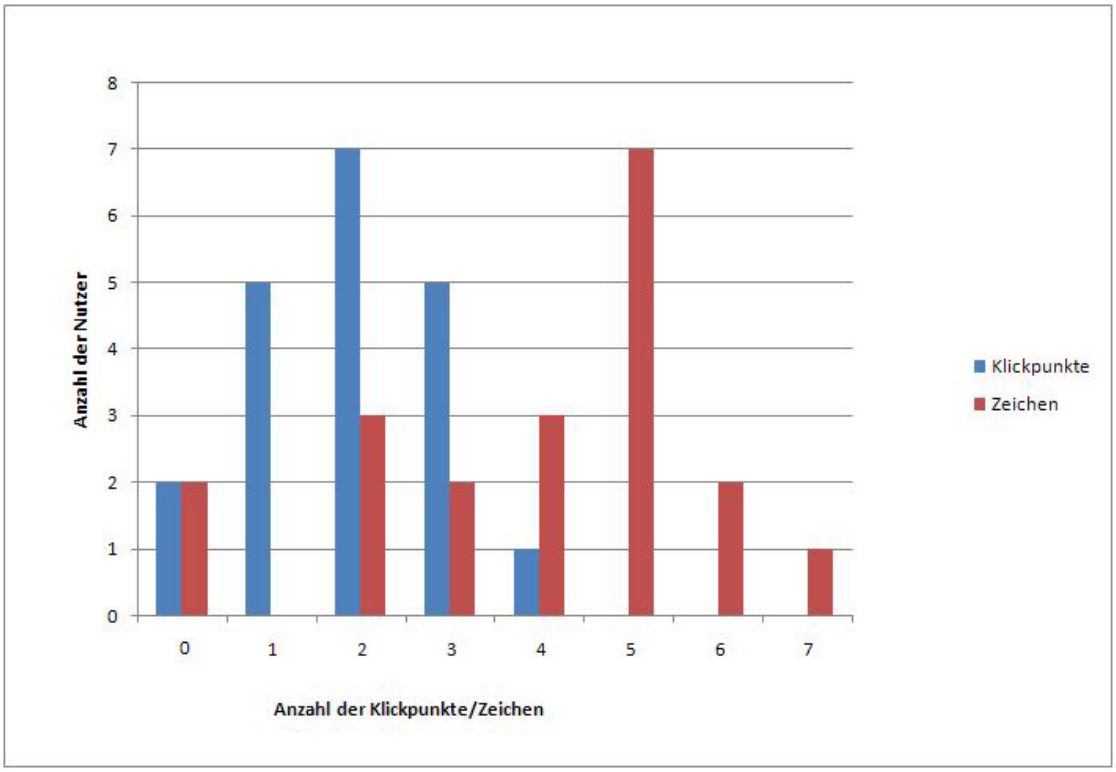

Abbildung 6.2: Anzahl der verwendeten Klickpunkte und Zeichen.

grafische Passworteingabe einen großen Wechsel der Eingabegeräte. Bei der hier vorgestellten Kombination hingeben wird ein ständiger Wechsel zwischen Maus und Tastatur vollzogen, für die Eingabe des Nutzernamens wird zuerst die Tastatur verwendet und bei der Passworteingabe wechselt es mehrfach zwischen Maus und Tastatur, abhängig vom gewählten Passwort. Sollte der Nutzer es gewohnt sein für die Eingabe mittels Tastatur beide Hände an diese zu legen, bedeutet es einen großen Mehraufwand für ihn, da er jedes Mal die Hand von der Maus zur Tastatur bewegt. Bei der Bedienung in der Form, das die rechte Hand an der Maus und die linke über der Tastatur verweilt, bedeutet es hingegen kaum einen größeren Aufwand zwischen Aktionen der rechte und linken Hand zu wechseln.

Die Zufriedenheit wird an Hand der Beeinträchtigungsfreiheit und Akzeptanz der Nutzung gemessen [23]. Die Nutzer, die den Fragebogen ausfüllten, gaben überwiegend an, dass sie es ansprechend finden zusätzlich zur Authentifizierung ein Bild nutzen zu können, siehe Abbildung 6.1. Durch den picture superiority effect [14] sollten die Nutzer in der Lage sein, sich zumindest den grafischen Anteil des Passwortes sowohl besser als auch länger merken zu können. Ausschließlich eine Testpersonen gab an, Bilder schlecht behalten zu können und deshalb das reine Textpasswort der Kombination vorziehen. Drei der Testpersonen wünschten sich die Möglichkeit individuelle Bilder verwenden zu können.

Alles in Allem ist es schwierig die Benutzerfreundlichkeit an Hand einer kleinen Test-

gruppe statistisch korrekt einzuschätzen. Eine neue Studie mit mindestens hundert Personen wäre hierfür angebracht, diese sollten dann in einem Labor beobachtest werden, um feststellen zu können, wie beispielsweise die Handhaltung bei der Eingabe ist oder um zu messen wie lange die Testpersonen fürs erstmalige Registrieren benötigen und wie viele Fehlversuche sie haben. Da allerdings 13 der 20 Befragten angaben, dass ihnen das neuartige Passwortsystem gefallen würde und von diesen sogar 12 es der herkömmlichen textuellen Passworteingabe vorziehen würden, lässt sich die Benutzerfreundlichkeit als höher bewerten.

6.2 Sicherheit

Wie bereits weiter oben erwähnt, ist ein Passwort um so sicherer, je länger es ist. Ein Passwort der Länge l hat eine Entropie von $l * \log_2 c$ Bits, falls die Zeichen zufällig sind und einem Alphabet von c Zeichen angehören. [3] Die Möglichkeit der Kombinationen beträgt dafür dann c^l. So hat beispielsweise ein normales Textpasswort, welches aus zufällig generierten 5 Zeichen besteht, diese bestehen aus Zahlen, Groß- und Kleinbuchstaben, eine daraus resultierende Entropie von $5 * \log_2 62 = 29,77$ Bits und $62^5 = 916132832$ Kombinationsmöglichkeiten. Bei einem Passwort, das mit Hilfe des hier vorgestellten Passwortsystems erzeugt wird, kommen zu den 62 Zeichen noch die 100 der zufällig im Bild verstreuten Klickpunktbereiche hinzu. Daraus ergibt sich dann bei ebenfalls 5 zufällig gewählten Zeichen in Kombination mit Klickpunkten eine Entropie von $5 * \log_2 162 = 36,7$ Bits und eine Anzahl von $162^5 = 111577100800$ Kombinationen. Bei angenommen einer Millionen Tastaturschläge pro Sekunde, welche ein Programm zum Rekonstruieren von Passwörtern hat, benötigt dieses für das Passwort, welches aus reinem Text besteht maximal ca. 15 Minuten. Bei dem Passwort, welches sowohl Text als auch Klickpunkte verwendet hingegen schon maximal ca. 31 Stunden. Im Vergleich dazu verbessert sich die Sicherheit bei längeren Passwörtern noch einmal erheblich. Bei einer Länge von 8 Zeichen ergibt sich für das textuelle Passwort eine Entropie von $5 * \log_2 62 = 47,6$ Bits, $62^8 = 218340105600000$ Kombinationsmöglichkeiten und eine Zeit von maximal ca. 7 Jahren. Bei der Kombination der textuellen und grafischen Passworteingabe ergeben sich hierfür folgende Werte: eine Entropie von $8 * \log_2 162 = 58,7$ Bits, eine Anzahl von $162^8 = 474373168300000000$ Kombinationen und eine Zeit von maximal ca. 15042 Jahre. Diese Beispiele zeigen, dass auf Grund der größeren Anzahl von 162 Zeichen bei der Kombination der grafischen und textuellen Passwortbestandteile die Sicherheit größer ist als bei herkömmlichen lexikografischen Passwörtern mit nur 62 Zeichen.

Die Teilnehmer der Umfrage verwendeten durchschnittlich zwei Klickpunkte und vier weitere Zeichen. Bei herkömmlichen textuellen Passwortsystemen, die hohe Anforderungen an die Sicherheit stellen wie zum Beispiel Internetbanking oder E-Mail Konten, wird eine Mindestlänge von acht Zeichen verlangt. Um also ein Passwort, welches eine Kombination aus grafischen und textuellen Bestandteilen darstellt, ebenfalls als sicher einzustufen, sollte es ebenfalls aus mindestens acht Zeichen bestehen. Dieses zu rekonstruieren würde dann auch maximal 15042 Jahre dauern. Die Anzahl der Klickpunkte

sollte auf mindestens drei und die Anzahl der Zeichen auf mindestens fünf festgelegt werden. Durch die Verwendung verschiedener Bilder auf den einzelnen Webseiten lässt die Mehfachnutzung von nur ein und demselben Passwort vermeiden, dies erhöht zusätzlich die Sicherheit.

6.3 Probleme und Risiken

Da Passwörter etwas sehr Geheimes sind, das außer dem Nutzer selbst keiner kennen sollte, es aber dennoch Menschen gibt, die versuchen werden, dieses zu rekonstruieren, wird die Verwendung von Passwörtern immer ein Risiko bleiben.

Zwei der Nutzer verwendeten auch gar keine Klickpunkte und nur Zeichen beziehungsweise ebenfalls zwei nutzten keine Zeichen und nur Klickpunkte. Um dies in der Zukunft zu vermeiden, sollte, wie bereits erwähnt, eine Mindestlänge des Passwortes festgelegt werden. Für die Mindestlänge sollten Klickpunkte auf drei und Zeichen auf fünf festgelegt werden. Die fünf Zeichen deshalb, da auf der einen Seite die Nutzer diese Anzahl zum Großteil selbst wählten und es auf der anderen Seite eine ausreichende Sicherheit bietet. Die Anzahl der Klickpunkte auf drei festzulegen, hat den Vorteil, das sich der Nutzer mit dem Bild beschäftigt und nicht nur einmal drauf klickt und somit diesen einen Klickpunkt schnell wieder vergisst. Auf der anderen Seite wären mehr als drei Klickpunkte zu viel, da die Nutzer dann dazu neigen ihre Punkte auf Linien oder nach anderen Mustern zu platzieren. [7]

Ein mögliches Risiko herkömmlicher textueller Passwörter ist Beispielsweise ein Keylogger, den es sowohl als Hardware- als auch als Softwareversion gibt und der dazu verwendet wird, die Eingaben über die Tastatur mitzuschreiben. Bei dem hier beschriebenen Programm ist dies nur bedingt möglich, da ein einfacher Keylogger nicht in der Lage ist, die Klickpunkte auf dem Bild zu protokollieren. Dadurch könnte zwar der textuelle Teil des Passwortes in falsche Hände geraten jedoch nicht der grafische.

Ein weiteres Risiko sind Shoulder-Surfing-Angriffe. Diese lassen sich durch das hier vorgestellte Programm zwar nicht vermeiden, aber stellen auch kein größeres Risiko dar als bei textuellen Passwörtern[8]. Einfache Passwörter, welche aus reinem Text bestehen, lassen sich vergleichsweise ähnlich gut mittels Shoulder-Surfing herausbekommen wie die Klickpunkte, die für die hier vorgestellte Authentifizierung verwendet werden. Da bei diesem System allerdings zu den Klickpunkten auch die textuelle Eingabe hinzukommt, dürfte der Angreifer Schwierigkeiten dabei haben, den schnellen Wechsel zwischen textueller und grafischer Eingabe mitzuverfolgen. Denn um alle Stellen des Passwortes zu erkennen, muss der Angreifer bei der textuellen Eingabe die Tastatur beobachten und bei der grafischen Eingabe den Bildschirm im Auge behalten. Wenn der Nutzer sein Passwort im Kopf hat und eine schnelle Eingabe erfolgt, wird der Angreifer bei einmaliger Beobachtung nicht in der Lage sein, das Passwort mittels Shoulder-Surfing zu erkennen.

Bei reinen grafischen Passwortsystemen ist die Anordnung der Klickpunkte zu einem Muster ein großes Problem [7,9]. Dies dürfte hier aber nicht so stark der Fall sein, da das Passwort nicht nur aus Klickpunkten besteht. Ein Muster in der Anordnung der Klickpunkte zu erkennen, ist nur dann möglich, wenn hinreichend viele Klickpunkte verwendet

werden, aber wie bereits weiter oben erwähnt, halte ich eine Durchschnittsanzahl von drei Klickpunkten für sinnvoll. Bei nur drei Klickpunkten lässt sich noch kein Muster erkennen.

Des weiteren könnte der Nutzer auf die Idee kommen und den textuellen Anteil nur als Beschreibung für die Klickpunkte zu verwenden, beispielsweise: „rotesAuto[Klick auf das rote Auto]“. Eine solche Wahl des Passwortes wäre nicht sehr sicher, da wie weiter oben beschrieben sich der textuelle Anteil des Passwortes mittels Keylogger ermitteln lässt und damit dann auch der Klickpunkt erraten werden kann.

Da bei dem hier vorgestellten Programm nur hundert verschiedene Klickpunkte existieren, siehe Abbildung 5.3, gibt es ein gewisses Maß an Falschakzeptanz im Bereich des grafischen Passwortanteils. Da die Bereiche zufällig bestimmt werden, kommt es vor, dass einige Bereiche sehr klein und andere hingegen sehr groß sind (siehe Abbildung 6.3). Dadurch kann es passieren, dass zwei Klickpunkte die retaiv weit auseinander liegen zum gleichen Bereich gehören (siehe die beiden rechten Punkte), wobei hingegen zwei nahe aneinander liegende Punkte zu unterschiedlichen Bereichen gehören (siehe die beiden linken Punkte). Bei einer Wahl der Klickpunkte nahe an diesen für den Nutzer unsichtbaren Bereichsgrenzen wird das Wiederholen und das spätere Einloggen Schwierigkeiten bereiten. Da der Nutzer beim Wiederholen seiner Klickpunkte leicht in den daneben liegenden Bereich klicken kann, wird sein Passwort nicht als korrekt anerkannt, dies führt zu mehrfachem Probieren und bedeutet damit einen hohen Zeitaufwand. Dieses Problem ist durch das Sichtbarmachen der Bereiche in Einloggphase leicht zu beheben.

Ein weiteres Problem bei der grafischen Passworteingabe sind Hotspots, siehe Abbildung 3.4 rechts. Diese Vorliebe für das Anklicken von bestimmten Bereichen liegt an der Wahl des Bildes. Am besten geeignet sind Bilder mit vielen Details und ohne große homogene Flächen, wie zum Beispiel der Himmel oder eine leere Straße. Vom Nutzer selbstgewählte Bilder würden zwar die Nutzerfreundlichkeit erhöhen und sicher auch zu einer besseren Merkbarkeit der Passwörter führen, dafür besteht dann allerdings keine Kontrolle mehr, ob die Bilder ausreichend viele Details haben.

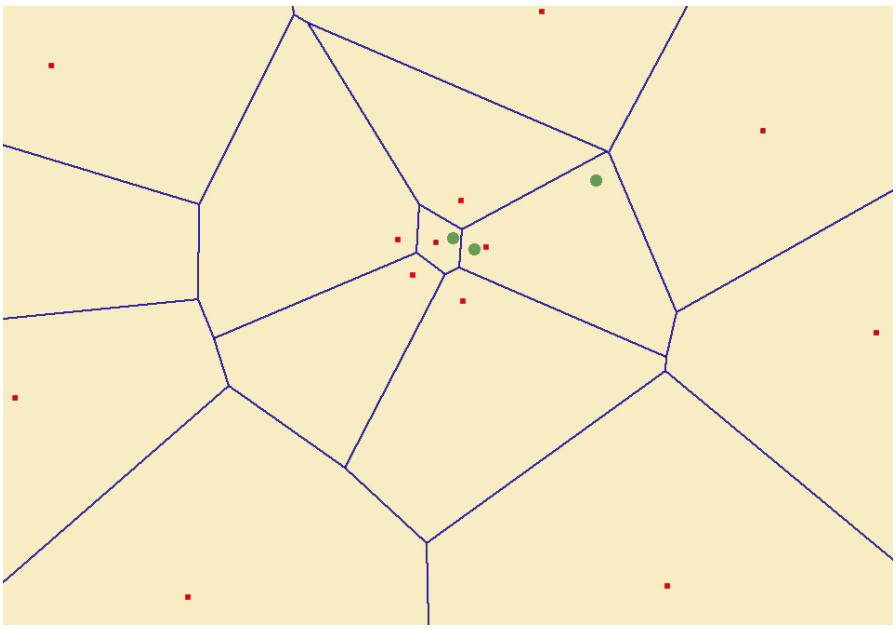

Abbildung 6.3: So könnten die Bereiche, dadurch, das sie zufällig angeordnet werden, auch verteilt sein. Die roten Punkte stellen die Position der Zufallswerte dar, die blauen Linien die Bereiche zu den jeweiligen Zufallswerten und die grünen Punkte mögliche Klickpunkte.

7 Zusammenfassung und Ausblick

Die hier vorgestellte Fusion grafischer und textueller Passwörter bietet als Grundlage die Registrierung und die Authentifizierung. Der grafische Anteil des Passwortes stellt durch die Unterteilung in Bereiche hundert neue Zeichen zur Erschaffung eines neuen Passwortes zur Verfügung. Durch diese größere Kombinationsmöglichkeit wird eine höhere Sicherheit gewährleistet. Durch die Verwendung eines Bildes zur Passwortgenerierung fühlt sich der Nutzer angesprochen und kann sich das Passwort sowohl besser als auch länger merken.

Zur Bewertung der Benutzerfreundlichkeit wurde eine Studie mit 20 Personen durchgeführt, diese ist nicht aussagekräftig und müsste für bessere statistische Auswertungen wiederholt werden. Dafür sollten mindestens hundert Teilnehmer unterschiedlichen Alters ausgewählt und in Laborbedingungen getestet werden. Um die Sicherheit noch weiter zu steigern, könnten für den grafischen Anteil drei Bilder zur Auswahl stehen, von denen der Nutzer das richtige auswählen muss. Zur Steigerung der Benutzerfreundlichkeit könnte die Möglichkeit bestehen, das Bild für den grafischen Anteil bei der Registrierung selber hochzuladen, wobei sich neue Angriffsmöglichkeiten ergeben könnten.

8 Referenzen

1. Karen Renaud und Antonella de Angeli, Visual Passwords: Cure-All or Snake-Oil?, 2009.

2. P.C. van Oorschot und Julie Thorpe, On Predictive Models and User-Drawn Graphical Passwords, 2008.

3. P.C, van Oorshot und Tao Wan, TwoStep: An Authentication Method Combining Text and Graphical Paswords, 2009.

4. K. M. Everitt, T. Bragin, J. Fogarty, T. Kohno, A Comprehensive Study of Frequenca, Interference and Training of Multiple Graphical Passwords, 2009.

5. S. Chiasson, A. Forget, E. Stobert, P. C. van Oorshot, R. Biddle, Multiple Passwords Interference in Text Passwords and Click-Based Graphical Passwords, 2009.

6. H. Tao, C. Adams, Pass-Go: Proposal to Improve the Usability of Graphical Passwords, 2007.

7. S. Chiasson, A. Forget, R. Biddle, P. C. van Ooorschot, User Interface design affects security: patterns in click-based graphical passwords, 2009.

8. F. Tari, A. A. Ozok, S.H. Holden, A Comparison of Perceived and Real Shoulder-surfing Risks between Aphanumerical and Graphical Passwords, 2006.

9. X. Suo, Y. Zhu, G. S. Owen, The Impact of Image Choices on the Usability and Security of Click Based Graphical Passworsds, 2009.

10. S. Schminke, M. Schott, C. Vielhauer and J. Dittmann, Evaluation of Fusion for Similarity Searching in Online Handwritten Documents, 2009.

11. E. Stobert, Usability and Strength in Click-based Graphical Passwords, 2010.

12. D. Fkorencio und C. A. Herly, A large –scale of the International password habbits. Prpceeding of the Imternational Conference on World Wide Web, (www2007), 657-666.

13. T. Scheider, M. Biermann, J. Dittmann, C. Vielhauer and K. Kümmel, Multi-biometric for Driver Authentification on the Example of Speech and Face, 2009.

14. S. Madigan, Picture memory. J.C. Yulille, Imaginery, Memory and Cognition: Essays in Honor of Allan Paivio. Erlbaum, Hillsdale, NJ, 1983, 66-89.

15. R. Dhamija und A. Déjà vu, A user study using Images for Authentification. Proceedings of the Conference on USENIX Security Symposium, (2000), 4-4.

16. I. Jermyn, A. Mayer, F. Monrose, M. Reiter und A. Rubin, The design and analysis of graphical passwords. In 8th USENIX Security Symposium, 1999.

17. S. Chiasson, R. Biddle, P. C. von Oorshot, A second look at the usability of click-based graphical passwords, In: ACM Symposium on Usable Privacy and Security (SOUPS), 2007.

18. J. Thorpe, P. C. van Oorshot, Human-seeded attacks and exploiting hot-spots in graphical passwords. In: 16th USENIX Security Symposium, 2007.

19. S. Chiasson, P. C. van Oorshot, R. Biddle, Graphical password authentification using Cued Click Points, In: European Symposium on Research in Computer Security (ESORICS), LNCS, vol. 4734, pp. 359-374, 2007.

20. S. Chiasson, A. Forget, R. Biddle, P. C. van Oorshot, Influencing Users Towards Better Passwords: Persuative Cued Click-Points, HCI 2008, British Society, 2008.

21. www.passfacespersonal.com (abgerufen am 28.5.2010)

22. www.wallpaper-page.eu (abgerufen am 13.6.2010)

23. Titel (deutsch): Ergonomische Anforderungen für Bürotätigkeiten mit Bildschirmgeräten - Teil 11: Anforderungen an die Gebrauchstauglichkeit; Leitsätze (ISO 9241-11:1998); Deutsche Fassung EN ISO 9241-11:1998, 1999.

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit ohne unzulässige Hilfe Dritter und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht.

Magdeburg, den 18.10.2010 Melanie Wetzel