Grafische Passwörter zur User-Authentifizierung auf mobilen Touch-Devices

Gernot Rottermanner, BSc.
University of Applied Sciences, St.Pölten
dm111539@fhstp.ac.at

Abstract

Sie nerven häufig und vergessen werden sie auch immer wieder: alphanumerische Passwörter. Zur besten Sicherheit sollen sie möglichst willkürlich aus Sonderzeichen, Zahlen und Ziffern bestehen. Aber manchmal stellt man sich die Frage, ob es nicht alternative Authentifizierungs-Methoden zum bekannten und weit verbreiteten Benutzername/Passwort-Pattern gibt und wie diese aussehen könnten. Dieses Paper befasst sich mit einer Alternative, das sogenannte grafische Passwort. Es werden Beispiele, Stärken und Schwächen in Bezug auf Usability und Sicherheit angeführt und analysiert.

1. Problemstellung

In einer groß angelegten Studie im Jahr 2007 haben Florêncio und Herley von *Microsoft Research* [1] untersucht, wie der tägliche Umgang mit Passwörtern im Web aussieht. Die Studie (sie lief über einen Zeitraum von drei Monaten und inkludierte mehr als eine halbe Million NutzerInnen der Windows Live Toolbar) zeigte auf, dass die BenutzerInnen im Durchschnitt im Besitz von 6,5 Passwörtern sind, die bei 25 Konten zum Einsatz kommen. Am Tag wurde acht Mal ein Passwort eingetippt. Das Passwort setzte sich mehrheitlich ausschließlich aus Kleinbuchstaben zusammen, außer es wurden Großbuchstaben oder Sonderzeichen ausdrücklich gefordert. Diese Zahlen zeigen deutlich, dass die Anzahl der Passwörter auf ein Minimum reduziert wird und ein und dasselbe Passwort bei mehreren Konten zum Einsatz kommt. Bei der Fülle an Konten wird es schlichtweg unmöglich, sich auch immer ein neues Passwort zuzulegen, das noch dazu einen gewissen Grad an Sicherheit bieten soll. Passwörter werden klarerweise umso sicherer, je willkürlicher eine Kombination aus Buchstaben, Zahlen und Sonderzeichen verwendet wird. Genau das ist aber ein Problem, den diese Kombinationen sind äußert kompliziert zu merken. Das menschliche Gehirn kann sich im Kurzzeitgedächtnis circa sieben willkürliche Zeichen merken, plus minus zwei Zeichen [2]. Sollen diese für längere Zeit im Gedächtnis behalten werden, dann müssen sich Passwörter zu einer persönlich sinnvollen Kombination zusammensetzen, etwa zu einem Wort oder bekannten Zahlenkombinationen. Deshalb neigen Menschen beim Zusammensetzen eines Passwortes schnell dazu, aus bekannten Wörtern, Buchstabenabfolgen und Zahlenkombinationen zu wählen und dieses Passwörter auch oft genug einzusetzen [2].

Die Technologiebranche erfährt durch das enorme Aufkommen von mobilen Endgeräten, im speziellen Smartphones, einen Umbruch. Das Smartphone gewinnt mehr und mehr an Bedeutung und wird zum ständigen Begleiter im alltäglichen Leben. Bei der Authentifizierung am mobilen Endgerät mithilfe eines alphanumerischen Passworts kommt daher auch ein Usability-Problem hinzu: Für die Eingabe fehlt meist eine physische Tastatur, sie muss daher auf einem kleinen Display abgebildet werden. Auch stehen sicherheitsrelevante Aspekte im mobilen Kontext an oberster Stelle, da die Gefahr, ein Passwort zu „erhaschen“, etwa in der U-Bahn und im öffentlichen Raum gegeben ist.

Das Paper greift daher in den folgenden Abschnitten Alternativen zur alphanumerischen Passworteingabe auf, die im Besonderen für mobile Endgeräte relevant sein könnten. Dabei werden die Möglichkeiten des grafischen Passworts näher erläutert und angeführt, welche Überlegungen und Beispiele in diesem Bereich bereits vorhanden sind. In diesem Zusammenhang werden auch die wichtigen Aspekte der Usability und Sicherheit aufgezeigt, die im Zusammenhang mit grafischen Passwörtern beachtet werden müssen.

2. Grafische Passwörter

Biddle et al [3] führen in ihrem Paper ein wesentliches Argument, das für grafische Passwörter

spricht, an: Das menschliche Gehirn hat sowohl eine ausgezeichnete Merkfähigkeit als auch ein gutes Erinnerungsvermögen für visuelle Information im Gegensatz zu verbaler Information. Die bekannteste Theorie dazu stammt von Allan Paivio. Er hat im Jahr 1971 die Theorie der doppelten Encodierung (*dual-coding theory*) entwickelt und vorgestellt. Das Gehirn besteht aus einem verbalen und einem non-verbalen System. Das verbale System ist für das Lesen und Hören von Begriffen, also für alle sprachlichen Informationen zuständig, das non-verbale für die Verarbeitung bildlicher Information. Die Doppelcodierung erhöht auch die Wahrscheinlichkeit, sich etwas besser zu merken. So werden etwa bei konkreten Wörtern wie „Haus“ oder „Auto“ beide Systeme angesprochen. Bei abstrakten Begriffen ist dies nicht der Fall (etwa Worte die man sich nicht vorstellen kann). Außerdem verarbeiten die Systeme Informationen auf unterschiedlicher Weise. Das non-verbale System arbeitet demnach schneller als das verbale [3].

Es gibt daher eine Reihe von Überlegungen, welche Alternativen es zum alphanumerischen Passwort geben kann, so etwa das unter dem Überbegriff stehende *grafische Passwort.* Im Wesentlichen können drei Arten von grafischen Passwörtern unterschieden werden [4]: *recall*, *recognition* und *cued-recall graphical passwords*. Ersteres zielt auf die Erinnerung ab, das heißt es wird ein Passwort definiert, das dann später immer wieder aus dem Gedächtnis abgerufen und eingegeben wird. Das klassische Text-Passwort zählt zu diesem Typ. *Recognition* bedeutet, etwas zu erfassen und zu erkennen. Bei dieser Methode etwa müssen BenutzerInnen aus einem Set von Bildern das richtige, bei der Passwort-Initialisierung definierte Bild erkennen. *Cued-recall* funktioniert ähnlich wie *recall*, nur das es zusätzlich bei der Abfrage einen Hinweis gibt, der bei der Eingabe auf die Sprünge helfen soll [3].

2.1. Recall-based graphical passwords

Bekanntestes Beispiel dieser Kategorie ist *Draw-A-Secret* (DAS, siehe Abbildung 1). DAS funktioniert folgendermaßen: Ein persönliches Passwort wird bei der Passwort-Initialisierung freihändig auf ein zweidimensionales Raster gezeichnet. Das Passwort kann dabei aus einem oder mehreren getrennten Strichen (welche mit sogenannten „Pen-Ups“ separiert sind) bestehen. Jede Rasterzelle, welche beim Zeichnen passiert wurde, wird als Koordinatenpaar encodiert abgespeichert. Für das in Abbildung 1 ersichtliche Passwort würde die encodierte Information lauten: (2,2), (3,2), (3,3), (2,3), (2,2), (2,1), (5,5). Das letzte Koordinatenpaar stellt das „Pen-Up“ dar.

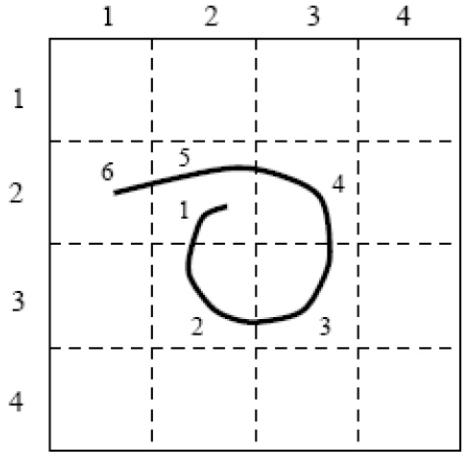

Abbildung 1: Beispiel DAS-Passwort

Es gibt wenig Information zur Usability oder Sicherheit der originalen DAS-Methode, lediglich wurde sie anhand eines Papier-Prototyps von Nali und Thorpe [5] getestet. Allerdings wurde diese Methode mehrfach adaptiert und weiterentwickelt [3]. Dunphy und Yan [6] erweiterten DAS dahingehend, dass zusätzlich ein Hintergrundbild angezeigt wird, welches die BenutzerInnen dazu ermutigen soll, komplexere Passwörter zu erstellen. Sie nannten diese Methode *BDAS (Background-Draw-A-Secret).* Allerdings zeigte sich, dass die Bilder gut gewählt sein müssen, um für diese Methode geeignet zu sein. Ein Bild mit zu viel Informationsgehalt wird sich schwer eignen, weil NutzerInnen wenig Anhaltspunkte haben, wo sie das Passwort zeichnen sollen. Die von den beiden Autoren durchgeführte Testreihe, die DAS mit BDAS verglich, zeigte auf, dass mithilfe der BDAS-Methode komplexere Passwörter erstellt wurden. Bei der Merkfähigkeit gab es allerdings keinen großen Unterschied zu DAS, teilweise war die Merkfähigkeit bei den Testpersonen, die DAS verwendet hatten, besser, was die Autoren damit begründeten, das die BDAS-Testpersonen auch komplexere Passwörter erstellten [6].

Als weiteres Beispiel kann an dieser Stelle *Pass-Go* genannt werden, welches ebenfalls auf *Draw-A-Secret* basiert. Tao und Adams [7] sahen ein Usability-Problem in der DAS-Methode: Wenn BenutzerInnen ein Linie zeichnen, die zu eng an einer Rasterlinie liegt, könnte es bei erneuter Eingabe zu hoher Fehleranfälligkeit kommen. Bei *Pass-Go* hingegen können BenutzerInnen ihre Linien nur durch Kreuzungspunkte zeichnen. Jeder Kreuzungspunkt ist dabei von einem unsichtbaren sensiblen Kreis

umgeben, damit BenutzerInnen den Kreuzungspunkt leichter erreichen können. Der Radius des sensiblen Kreises ist ¼ der Größe einer einzelnen Rasterzelle. Als Information wird dann immer das Koordinatenpaar eines Kreuzungspunktes im 2-dimensionalen Raster gespeichert. Das Passwort kann sich aus einer Kombination von Strichen und Punkten zusammensetzen (siehe Abbildung 2).

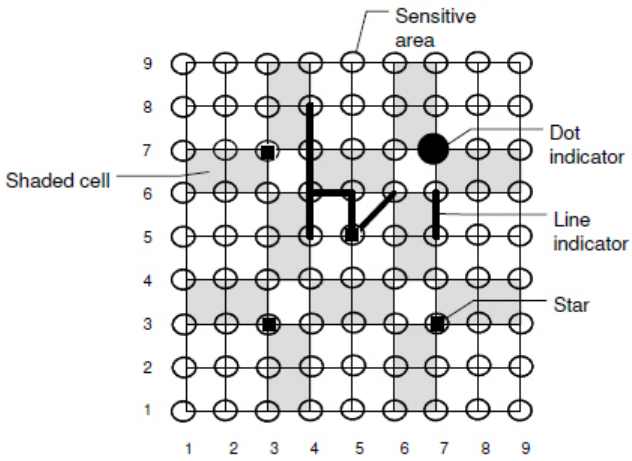

Abbildung 2: Pass-Go

Pass-Go wurde auch in einer größeren Feld-Studie mit 167 Personen in einem Zeitraum von drei Monaten getestet. Es wurden 6800 Login-Versuche aufgezeichnet, 5291 davon waren erfolgreich, die Erfolgsrate lag demnach bei 78%. Die Studie zeigt auch, dass die Rate an erfolgreichen Logins in der ersten Woche noch geringer war (ca. 65%), in der dreizehnten Woche aber auf über 90% anstieg [7]. Die Methode von Pass-Go ist vor allem deshalb relevant, da eine Mini-Variante von Pass-Go in das mobile Betriebssystem Android integriert wurde. Hier kommt eine stark vereinfachte Variante mit einem 3x3 Raster mit 9 Rasterkreuzungen beim „Screen-Unlock“ des Gerätes zum Einsatz, der optional eingestellt werden kann [3].

In diesem Zusammenhang sei auch das neue Bildkennwort in der sogenannten *Consumer Preview* von *Windows 8* angeführt, da es ein weiteres Beispiel dafür ist, dass grafische Passwörter teilweise auch Einzug in den Massenmarkt gefunden haben. Die Vorab-Version von *Windows 8* stellt eine radikale Veränderung im Vergleich zu den Vorgängern dar, da es vor allem für mobile Endgeräte mit Touch-Display optimiert wurde. Vom Prinzip her ist das Bildkennwort in Windows 8 dem *BDAS* ähnlich, da auch bei dieser Methode ein persönliches Bild als Untergrund verwendet wird, wo dann gewisse Elemente darauf gezeichnet werden sollen, um sich beim System (in diesem Fall bei Windows 8) zu authentifizieren. Allerdings stehen keine Freihandzeichnungen, sondern nur drei Gesten zur Verfügung: Punkt, Linie und Kreis (siehe Abbildung 3). Dieser Schritt resultiert daraus, dass auch Freihandgesten getestet wurden, allerdings dauerte die Anmeldung zu lange. Stellt man den BenutzerInnen nur eine eingeschränkte Anzahl an Gesten zur Verfügung, ist die Anmeldung um ein Drittel schneller als bei Freihandgesten [8]. Als weitere Stärke dieser Methode wird angegeben, dass die Richtung sowie Start- und Endpunkt der Geste entscheidend sind und diese bei der Authentifizierung eingehalten werden muss, da sie sonst fehlschlägt.

Abbildung 3: Bildkennwort bei Windows 8

Die Methode des Bildkennworts funktioniert zusammengefasst folgendermaßen: Das gewählte Bild wird in ein Raster in 100 Abschnitte unterteilt. Wie bei DAS werden die einzelnen Punkte durch die Koordinaten x,y definiert. Bei Linien werden die Start- und Endkoordinaten gespeichert, so kann ermittelt werden, in welche Richtung die Linie gezogen wurde. Bei Kreisen werden der Mittelpunkt, der Radius und die Richtung gespeichert. Bei der dritten Geste, dem Punkt werden lediglich die Koordinaten selbst gespeichert. Bei der Anmeldung werden die Unterschiede jeder einzelnen gezeichneten Geste mit der gespeicherten Geste ermittelt. Anhand der Gesamtabweichung wird dann ermittelt, ob die Authentifizierung erfolgreich war oder nicht [8].

2.2. Recognition-based graphical passwords

Bei dieser Methode werden BenutzerInnen üblicherweise beim Erstellen des Passworts nach einer gewissen Anzahl von Bildern gefragt, aus denen sie wählen sollen. Diese Bilder werden dann als *key images* definiert. Bei der Authentifizierung selbst

müssen die BenutzerInnen aus einer Reihe von bedeutungslosen Bildern (*decoy images)* die *key images* erkennen und diese auswählen. Werden die Richtigen ausgewählt, ist die Authentifizierung erfolgreich. Je nach Implementierungsform können AnwenderInnen die *key images* aus den eigenen, persönlichen Bildern auswählen oder vom System vorgegebene Bilder nutzen. Die Vor- und Nachteile dieser beiden Varianten werden dann später erläutert. Bekanntestes Beispiel für ein *recogintion-based graphical password* ist *Passfaces*, welches auch als kommerzielles Produkt besteht und bei Online-Applikationen eingesetzt werden kann [9]. Bei dieser Methode werden aus einem Set von Bildern *key images* ausgewählt. Die Authentifizierung selbst besteht aus mehreren Runden, die zu bestehen sind (beispielsweise vier). In jeder Runde wird ein Panel von neun Bildern angezeigt, eines davon ist das persönliche *key image*, das erkannt werden soll. Alle Runden müssen fehlerfrei absolviert werden, damit die Authentifizierung erfolgreich ist. Wie der Name schon sagt, werden bei *Passfaces* Gesichter von Personen verwendet. Der Grund dafür ist, dass sich der Mensch Gesichter besonders gut merken kann. Wie bereits erwähnt, ist die rechte Hälfte des menschlichen Gehirns für die Verarbeitung von Bildern zuständig. Wenn Personen Gesichter sehen, ruft das erhöhte Gehirnaktivitäten in gewissen Bereichen der rechten Gehirnhälfte hervor [10]. Gesichter werden demnach anders verarbeitet als Objekte oder Bilder.

2.3. Cued-recall graphical passwords

Bekanntestes Beispiel in dieser Kategorie ist *PassPoints*. Hierbei gibt es ein vom System vorgegebenes Bild, auf das man dann seine sogenannten *click-points* setzen soll, typischerweise sind es fünf. Bei der Authentifizierung muss man dann wieder die gewählten Stellen in der richtigen Reihenfolge anklicken, als *Cue* dient ein Starthinweis. Eine Testreihe ergab, dass die BenutzerInnen 64 Sekunden zum Erstellen eines Passwortes brauchten, weitere 171 Sekunden Trainingszeit, dafür aber rund 9-19 Sekunden zum erfolgreichen Login [3].

3. Grafische Passwörter: Usability und Sicherheit

Biddle et al [3] merken an, dass es zu den wenigsten der genannten Beispiele fundierte Studien zur Benutzbarkeit und Sicherheit gibt. Und wenn sie vorhanden sind, dann werden keine einheitlichen Kriterien verwendet, um die Methoden zu vergleichen. Deshalb empfehlen Biddle et al [3], dass einheitliche Kriterien aufgestellt werden sollen, um die Methoden auch gut miteinander vergleichen zu können, um die Unterschiede in Effizienz und Benutzbarkeit gegenüber text-basierten Passwörtern aufzuzeigen.

3.1. Aspekte der Usabiltiy bei grafischen Passwörtern

Wichtig beim Einsatz von grafischen Passwörtern wird es sein, die eigene Zielgruppe zu kennen. Grafische Passwörter sind noch nicht weit verbreitet, daher wird die Rolle des Vertrauens in das neue System eine wichtige Komponente sein. Des Weiteren wird von BenutzerInnen ein gutes Sehvermögen, Farbsehen und meistens auch Geschicklichkeit - wenn wir das Beispiel mit Gesteneingaben hernehmen - abverlangt. Außerdem wird jedes neue System eine gewisse Trainingsphase mit sich ziehen. Die BenutzerInnen müssen gewisse Geduld mitbringen [3].

Ein weiterer Parameter ist, wie häufig der Login verwendet wird. Wird der Login oft benötigt, ist es wichtig, dass er einfach durchzuführen ist. Dafür kann das Passwort auch etwas komplexer sein, da es häufig benötigt wird und demnach fester im Gedächtnis verankert ist. Jedenfalls muss der Login-Prozess schnell voran gehen. Dunphy et al [4] haben etwa in ihrer Studie, in der sie einen Nachbau ähnlich *Passfaces* testeten, festgestellt, dass der Login zu lange dauerte und diese Art von Login bei einer Dauer länger als 20 Sekunden unattraktiv wurde. Wird ein Login nicht oft benötigt, muss er leicht zu merken sein.

Aufgrund dieser Merkmale können schon einige Usability-Parameter aufgestellt werden, die auch bei einem Test herangezogen werden sollen [3]:

- Die Dauer, um ein Passwort zu erstellen
- Die Dauer, um sich einzuloggen
- Die „Einprägsamkeit“: Diese kann vor allem durch die Erfolgsrate und der Anzahl an Fehlern ermittelt werden. Für diesen Punkt müssen auch standardisierte Zeitpunkte festgelegt werden, beispielsweise die Erfolgsrate nach 3 Wochen.

3.1.1. Passwort-Initialisierung

Vor allem bei grafischen Passwörtern der Kategorie *recoginition-based* stellt sich die Frage, ob BenutzerInnen aus dem persönlichen Bildbestand *key images* auswählen sollen, oder ob die Bilder vom Betreiber selbst kommen. Dieser Faktor hat auch schon wesentliche Auswirkungen auf die Usability. Werden Bilder aus einem persönlichen Bildbestand ausgewählt,

werden sie auch leichter gemerkt, weil von Haus aus eine emotionale, persönliche Bindung besteht. Dem gegenüber stehen aber wieder einige Gefahren. So zeigte sich etwa in der Studie von Dunphy et al [4], dass Bilder aus dem eigenen Bildbestand der BenutzerInnen erst nach gewissen Kriterien überprüft werden müssen, damit sie als verwendbar eingestuft werden können. Weniger brauchbar sind zum Beispiel Bilder, die wenig oder zu viel Bildinformationen beinhalten, oder die zum Beispiel zu dunkel sind und auch Bilder, die sich zu ähnlich sind. In der Testreihe wurde dafür die Methode der *canny edge detection* verwendet. Diese Technik extrahiert die Bereiche des Bildes, wo sich die Helligkeit stark ändert. Das Resultat ist ein binäres Bild aus schwarzen und weißen Pixeln, wobei die weißen Pixel die Ecken darstellen. Mithilfe einer Formel wird dann berechnet, ob die Anzahl der Ecken und damit die Bildinformation vertretbar sind oder nicht [4].

Ein weiteres Problem beim Einsatz von eigenen Bildern kann sein, dass wieder die Gefahr besteht, dass sie wiederverwendet werden, auch bei anderen Services. Das fällt weg, wenn BenutzerInnen aus einem vom System vorgegeben Pool an Bildern auswählen müssen. Das wiederum hat den Nachteil, dass die Trainingsphase länger dauert, da die Bilder völlig unbekannt sind [3].

Abschließend stellt sich noch die Frage, ob BenutzerInnen ihre *key images* selbst auswählen sollen, oder ob sie einfach in der Trainingsphase automatisiert zugeteilt werden. Wie sich in einer Studie herausstellte, können Personen bei einer selbstständigen Auswahl an Gesichtern dazu tendieren, eher attraktive und weibliche Gesichter zu wählen, was Einfluss auf die Sicherheit des Passworts hat [11].

3.1.2. Login

In Studien, wo grafische Passwörter getestet wurden, wird immer wieder der Parameter des erfolgreichen Logins untersucht, dabei wird aber sehr unterschiedlich vorgegangen. Die eine Studie misst die Erfolgsrate bei drei Login-Versuchen, die andere bei einem Login-Versuch. Außerdem wird bei den meisten Studien davon ausgegangen, dass die BenutzerInnen sich nur ein Passwort merken müssen, obwohl dies kaum der Realität entsprechen dürfte. Müssen sich BenutzerInnen mehrere Passwörter einprägen, hat das Einfluss auf die Erfolgsrate beim Login, man spricht in diesem Fall von *Interferenz*. Sind also zwei Passwörter zu ähnlich, können sie schnell verwechselt werden. Dieser Faktor muss bei einer Evaluierung einer Passwort-Methode ebenfalls berücksichtigt werden, meinen etwa Everitt et al [11], die diesbezüglich eine Testreihe durchgeführt haben. 100 Testpersonen wurden in einem Zeitraum von fünf Wochen ein bis vier Mal pro Woche per E-Mail dazu aufgefordert, sich bei mehreren für den Testzweck erstellte Webseiten zu authentifizieren. Insgesamt kamen vier unterschiedliche Passwörter, die jeweils einer Webseite zuzuordnen sind, für jede Testperson zum Einsatz. Erwähnenswert dabei ist, dass Testpersonen, die vier verschiedene Passwörter einer Woche auf einmal benutzen, eine 10-mal höhere Fehlerrate auswiesen als Testpersonen, die nur ein Passwort benutzten.

3.1.3. Passwort vergessen

Auffallend ist, dass der Fall, ein Passwort zu vergessen und ein neues anzufordern bei Usabiltiy-Tests von grafischen Passwörtern, meistens außer Acht gelassen wird. Bekanntermaßen kann ein neues Text-Passwort relativ einfach per Mail oder Telefon übermittelt werden. So wird man beim grafischen Passwort auch über einen zweiten Weg ausweichen müssen, etwa durch ein Text-Passwort als Fallback-Lösung oder eine URL, mit der es möglich ist, ein neues grafisches Passwort anzulegen [3].

Abschließend sei noch erwähnt, dass es beim Einsatz eines grafischen Passwortes vor allem auf die *Domäne* ankommt, für hochsichere Anwendungen ist auch das höchste Maß an Sicherheit wichtig, hier wird man nicht daran vorbei kommen, auch komplexere Passwörter zu erstellen, was negative Auswirkungen auf die Usability hat. Bei weniger sicherheitsrelevanten Services kann auch die Sicherheitsstufe geringer sein, dafür soll die Usability an oberster Stelle stehen. Beide Faktoren vollständig abzudecken, wird eher unwahrscheinlich sein [3].

3.2. Aspekte der Sicherheit

Höchstes Ziel soll bei Passwörtern sein, dass sie auch ein hohes Maß an Sicherheit bieten. Neben den allgemein bekannten Attacken - etwa *Phishing* oder *social engineering* - gibt es im Kontext der mobilen Nutzung auch gesonderte Gefahren, die hohe Aufmerksamkeit verdienen sollten: Etwa *shoulder surfing* oder sogenannte *smudge attacks.* Zweiteres hat für breites Aufsehen gesorgt. Ein Nebeneffekt bei der Bedienung von Touchscreens ist, dass fettige Rückstände der Finger am Display haften bleiben, diese Spuren bleiben ersichtlich. Aviv et al [12] zeigten in ihrer Testreihe auf, dass dies ein relevantes Sicherheitsproblem darstellen kann. Tests wurden an der bereits erwähnten Screen-Unlock-Funktion bei

Android-Smartphones durchgeführt. Es stellte sich heraus, dass die Forscher in der Lage waren, in 92% der Fälle das Entsperr-Muster anhand der Rückstände zumindest teilweise zu rekonstruieren, vollständig sogar bei 68% der Fälle mit entsprechender Aufzeichnung mit Kamera und darauffolgenden Bildbearbeitungs-Techniken. Die Studie zeigt, dass Touchscreen-Displays ein echtes Sicherheitsproblem darstellen können. Allerdings unter der Voraussetzung, dass das Entsperr-Muster auch in gewisser Weise noch ersichtlich ist. Wird das Display gesäubert, ist diese Technik dann nicht mehr oder nur schwer einsetzbar.

In diversen Studien [2–4] zu grafischen Passwörtern ist immer wieder von *shoulder surfing* die Rede. Das bedeutet, dass der Angreifer versucht, die Passwort-Eingabe „über die Schulter“ mit zu verfolgen. Bei Text-Passwörtern ist es daher gängige Praxis, die Eingabe im Eingabefeld durch Punkte zu verschleiern. Schwieriger wird dies aber Passwörtern der Kategorie *recognition-based.* Es gibt zwar Möglichkeiten gegen solch ein Szenario des *shoulder surfings*, jedoch immer auf Kosten der Usability, Logins dauern schlichtweg länger und sind weniger effizient. So ist es beispielsweise relativ einfach zu realisieren, dass bei jedem neuen Authentifizierungsversuch auch die *key images* an einer anderen Position aufscheinen. Allerdings wird genau in diesem Fall die Merkfähigkeit beeinträchtigt, weil es sonst möglich wäre, sich neben dem Bild selbst auch die Position des *key images* einzuprägen.

4. Fazit

Die Beispiele zeigen deutlich, dass es bereits viele Überlegungen für Alternativen zu alphanumerischen Passwörtern gibt, ein paar Methoden sogar schon großflächig eingesetzt werden. Es zeigt sich aber auch, dass diese Methoden teils sehr unterschiedlich evaluiert werden. Außerdem stellt sich die Frage, für welchen Verwendungszweck grafische Passwörter geeignet sind. Wie die Beispiele zeigen, sind grafische Passwörter bei der Authentifizierung am mobilen Endgerät selbst beliebt. Wie sieht es aber bei der Authentifizierung bei Web-Services aus? Unter welchen Umständen kann hier das grafische Passwort sicherer oder einfacher zu merken sein, als das alphanumerische Passwort? Ein Problem liegt sicherlich noch darin, dass derzeit keine Studien vorliegen, in denen deutliche Vorteile gegenüber textbasierten Passwörtern nachgewiesen wurden. Laut Biddle et al [3] ist es daher unumgänglich, grafische Passwörter mittels standardisierter Kriterien zu testen, um sie auch bestmöglich mit alphanumerischen Passwörtern vergleichen zu können. Abschließend sei erwähnt, dass bereits jetzt große Unternehmen wie Microsoft oder Google vorzeigen, dass das grafische Passwort gute Chancen hat und breite Anwendung finden kann, da es bereits in den Betriebssystemen Windows 8 und Android implementiert wurde.

5. Referenzen

[1] D. Florencio und C. Herley, „A large-scale study of web password habits“, 2007, S. 657.

[2] J. Yan, A. Blackwell, R. Anderson, und A. Grant, „Password memorability and security: empirical results“, *IEEE Security & Privacy Magazine*, Bd. 2, Nr. 5, S. 25–31, Sep. 2004.

[3] R. Biddle, S. Chiasson, und P. van Oorschot, „Graphical Passwords: Learning from the First Twelve Years“. [Online]. Available: http://www.scs.carleton.ca/research/tech_reports/index.php?abstract=TR-11-01&Year=2011. [Accessed: 29-März-2012].

[4] P. Dunphy, A. P. Heiner, und N. Asokan, „A closer look at recognition-based graphical passwords on mobile devices“, 2010, S. 1.

[5] D. Nali und J. Thorpe, „Analyzing User Choice in Graphical Passwords“, 2004. [Online]. Available: http://www.cs.carleton.ca/research/tech_reports/2004/. [Accessed: 01-Mai-2012].

[6] P. Dunphy und J. Yan, „Do background images improve ‚draw a secret‘ graphical passwords?“, 2007, S. 36.

[7] H. Tao und C. Adams, „Pass-Go: A Proposal to Improve the Usability of Graphical Passwords“. International Journal of Network Security, Vol.7, No.2, PP.273–292, Sept. 2008.

[8] S. Sinofsky, „Anmelden mit Bildkennwort - Die Entwicklung von Windows 8 - Site Home - MSDN Blogs“, 22-2011. [Online]. Available: http://blogs.msdn.com/b/b8_de/archive/2011/12/22/anmelden-mit-bildkennwort.aspx. [Accessed: 31-Dez-2011].

[9] Passfaces, „Two Factor Authentication, Graphical Passwords - Passfaces“. [Online]. Available: http://www.realuser.com/enterprise/products/products.htm. [Accessed: 10-Apr-2012].

[10] „The Science behind Passfaces“. 2011.

[11] K. M. Everitt, T. Bragin, J. Fogarty, und T. Kohno, „A comprehensive study of frequency, interference, and training of multiple graphical passwords“, 2009, S. 889.

[12] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, und J. M. Smith, „Smudge Attacks on Smartphone Touch Screens“. .