H. Reiterer & O. Deussen (Hrsg.): Mensch & Computer 2012
München: Oldenbourg Verlag, 2012, S. 273-282

VidPass – Passwörter in Raum und Zeit. Zur Usability von Videopasswörtern

Stefan Penninger[1], Tim Schneidermeier[2], Hannes Federrath[3], Christian Wolff[2]

Fakultät für Wirtschaftswissenschaften, Universität Regensburg[1]
Institut für Information und Medien, Sprache und Kultur (I:IMSK), Universität Regensburg[2]
Fachbereich Informatik, Universität Hamburg[3]

Zusammenfassung

Textbasierte Benutzerauthentikation mit Passwörtern bringt häufig Usability-Probleme mit sich. Grafische Passwörter versuchen die Authentikation benutzerfreundlicher zu gestalten. Diese beschränken sich in der Regel auf statische Bildelemente, die von menschlichen Nutzern aktiv erstellt oder passiv wiedererkannt werden müssen. Der *Picture Superiority Effect* geht davon aus, dass sich Menschen grafische Konzepte leichter merken und wiedergeben können, als dies bei textuellen Passwörtern der Fall ist. Die vorliegende Studie erweitert diesen statischen Ansatz um eine dynamische Komponente und stellt erstmalig ein videobasiertes Passwortverfahren vor. In einer Nutzerstudie wurde festgestellt, dass der vorgestellte Ansatz zwar einfach in der Bedienung ist, zur Erhöhung der Nutzerakzeptanz allerdings noch weiterer Optimierung bedarf.

1 Motivation

Benutzbare und sichere Authentikation ist durch die Vielzahl zugangsgeschützter Systeme – in der Realwelt ebenso wie auf Computersystemen – immer wichtiger geworden. Historische Beispiele hierzu existieren seit der Erfindung des ersten (physischen) Schlüssel-Schloss-Paares oder in der Verwendung von Losungen und Parolen bereits in der frühen Militärgeschichte (Bauer 2000; Singh 2000). Seit der Verbreitung von Vernetzung von IT-Systemen geschieht die Benutzerauthentikation zumeist nicht mehr zwischen zwei Personen, sondern zwischen einem Computersystem und der Person, die sich als legitimer Benutzer ausweisen will. Das klassische Authentisierungsverfahren ist die Benutzername-Passwort-Kombination. Dieses Verfahren ist als sehr sicher einzuschätzen, eine ausreichende Passwortlänge und –struktur vorausgesetzt. Mit zunehmender Rechenkapazität und Geschwindigkeit von angreifenden kryptoanalytischen Systemen nimmt jedoch die für die Sicherheit des Verfahrens notwendige Komplexität immer mehr zu. Ausreichend „kryptische“ Passwörter sind für den

Benutzer schwer im Gedächtnis zu behalten und gelten daher als wenig benutzerfreundlich (Wood & Banks 1993; Kim-Phuong et al. 2007). Der Widerspruch zwischen sicheren, kryptischen Passwörtern und den kognitiven Fähigkeiten von Benutzern, diese zu memorieren, verdeutlicht die Notwendigkeit von benutzerfreundlichen Authentisierungssystemen. In der vorliegenden Arbeit wird daher anhand einer prototypischen Umsetzung ein Konzept zur Kombination von grafischen Passwörtern mit einer temporalen Komponente vorgestellt. Eine Nutzerstudie zeigt darüber hinaus Usability-, Akzeptanz- und Sicherheitsaspekte des Systems in der Benutzung durch konkrete Testpersonen auf.

2 Grundlagen von Authentikationssystemen

Authentikation bezeichnet die korrekte Zuordnung einer Identität zu einem Subjekt, unabhängig davon, ob dies einen Menschen, einen Dienst oder ein Gerät betrifft. Im konkreten Fall der Benutzerauthentikation bedeutet dies eine eindeutige Identifikation beziehungsweise eine Identitätsfeststellung des Benutzers an einem Computersystem (Federrath & Pfitzmann 2006). Verbunden mit dieser Identität ist die Gewährung von speziellen Privilegien oder Rechten in dem betreffenden System: Die Benutzung eines Computers an sich (Anmeldung am Betriebssystem), Schreib- oder Leserechte auf Informationen (Dateien), Freigabe von Transaktionen (Online-Banking) bis hin zur Inanspruchnahme von sensiblen Diensten (elektronischer Personalausweis, elektronische Gesundheitskarte oder Steuererklärung). In manchen Ländern werden bereits elektronische Wahlsysteme angeboten (beispielsweise in Estland (Madise 2006). Benutzerauthentikation ist somit eines der zentralen Themen der IT-Sicherheit und für die Teilnahme an umfangreichen Aspekten des modernen Lebens unabdingbar. Die Identität eines Benutzers wird anhand von speziellen, personenbezogenen Merkmalen nachgewiesen (Klingler 2011). Diese werden in drei Klassen unterteilt: Wissensbasiert (also durch Kenntnis eines Passworts oder einer Losung), Besitzbasiert (durch Besitz eines Gegenstands wie etwa einer Smartcard) oder durch biometrische Merkmale (wie Fingerabdruck oder Retinaabbild). Weitere Authentikationsverfahren überprüfen nicht ausschließlich die eindeutige Zuordnung einer Person zu einer Identität. CAPTCHA-Systeme (*Completely Automated Public Turing test to tell Computers and Humans Apart*, vgl. Penninger et al. 2012) etwa testen, ob das anmeldende Subjekt generell menschlich ist und nicht ein automatisches Anmeldeskript eines Spammers.

3 Usability und Security: Gegensätze oder Abhängigkeit

Usability stellt einen wichtigen Faktor für sichere Authentikationsmechanismen dar. Gerade bei textbasierten Passwörtern greifen Nutzer zu Gunsten der Memorierbarkeit oft auf einfache und daher vorhersehbare Losungen zurück (vgl. Florencio & Herley 2007). Es entsteht eine Diskrepanz zwischen sicheren und benutzerfreundlichen Lösungen: Entweder die gewählten Passwörter sind unsicher, aber leicht zu erinnern, oder aber sicher, dafür kaum erinnerbar (Sasse et al. 2001). Bei passwortgestützten Authentikationssystemen konnten in Un-

tersuchungen eine Abhängigkeit von Usability und Security-Aspekten nachgewiesen werden (Hub et al. 2010).

Einen Ausweg aus diesem Dilemma versprechen grafikbasierte Authentikationsmechanismen, die mit Hilfe direkter Manipulation (Mausklicks) bedient werden (Biddle et al. 2009; Wiedenbeck et al. 2005; Jansen et al. 2003; Klingler 2011): Passwörter werden dabei durch Klicks auf frei wählbare Punkte in einem oder mehreren Bildern gesetzt. Für eine erfolgreiche Authentikation gilt es, die gesetzten Klicks zu wiederholen. Grafische Passwörter machen sich vor allem den so genannten *Picture Superiority Effect* zu Nutzen, der besagt, dass sich das menschliche Gehirn an Bilder im Vergleich zu Text oder anderen syntaktischen oder semantischen Items genauer und besser erinnern kann (Childers & Housten 1984; DeAngeli et al. 2005; Jermyn et al. 1999). Studien haben gezeigt, dass sich tatsächlich eine Steigerung der Usability durch grafische Passwörter erreichen lässt (Chiasson et al. 2008; Moncur & Leplâtre 2007; Hinds & Ekwueme 2007). So wurde beispielsweise in einer Studie nachgewiesen, dass grafische Passwörter wesentlich effektiver behalten werden können (Moncur & Leplâtre 2007).

Die hier vorliegende Studie greift die positiven Ergebnisse grafischer Passwörter hinsichtlich Usability auf und erweitert diese um eine temporale Komponente: anstelle von statischen Grafiken wird eine Videosequenz für das Erstellen und Eingeben einer vierstelligen Passwortkombination verwendet. Der Identifikationsschlüssel wird vom System auf Übereinstimmung in Raum und Zeit überprüft bevor die Authentikation festgestellt wird. Ziel ist es zu überprüfen, welche Auswirkungen sich bezüglich Usability und Sicherheit ergeben. Es wird angenommen, dass ähnlich gute Usability-Ergebnisse mit diesem Ansatz erreicht werden können wie bei statischen bildbasierten Verfahren und gleichzeitig die Sicherheit verbessert werden kann.

4 Videobasierte Authentikation: Ein Prototyp

Der Prototyp einer videobasierten Passwortauthentikation baut auf dem Hintereinanderschalten mehrerer Bildidentifikationsakte auf, d. h. der Benutzer klickt mehrfach in das Video, um Zuordnungen zu treffen. Dabei sind verschiedene Vorentscheidungen zu treffen: Das Video sollte nicht länger als 30 Sekunden sein. Diese Zeitspanne wurde gewählt, um einerseits eine ausreichende Passwortentropie (Maus 2008) gewährleisten zu können, und andererseits den Authentikationsvorgang nicht zu lang werden zu lassen. So sollen Effizienz des Verfahrens und die damit verbundene *User Experience* gewährleistet werden. Die Anzahl an Szenenwechseln sollte zudem nicht zu groß werden, um den Benutzern die Möglichkeit zu geben, die von ihnen zu wählenden Klickpositionen ausreichend bequem zu setzen. Zu schnelle Schnitte und zu viele Szenenwechsel erhöhen die kognitive Belastung bis hin zur Unbenutzbarkeit. Ein weiteres Merkmal ist die Anzahl an markanten Stellen im Video. Diese sollten möglichst zahlreich sein, um das Spektrum der möglichen Klickstellen und damit die Passwortstärke zu erhöhen. Auch die Bekanntheit des Videos wird als Kriterium mit einbezogen. Ein unbekanntes Video führt zu einer deutlich längeren Phase der Passworterstellung, da das Video mehrere Male zusätzlich betrachtet werden muss. Dieser Kriterienkatalog führte zur Auswahl der ersten 25 Sekunden des Vorspanns der TV-Zeichentrickserie *Die Simpsons* als

Testvideo, da dieses einem breiten Personenkreis bekannt und somit für den Test geeignet ist. Ein früher Pretest mit einer geringen Anzahl von Teilnehmern lieferte zusätzliche Designhinweise: So wurde die Anzahl der zu setzenden Klicks auf vier festgelegt, welche sich in der Abspieldauer von 25 Sekunden als guter Kompromiss zwischen Sicherheit (in Bezug auf die Passwortentropie) und Benutzbarkeit (durch geringe Dauer) zeigten. Die Rastergröße wurde mit 20 mal 20 Feldern (bei einer Videoauflösung von 480 mal 320 Pixel) als praktikabelste Lösung bewertet.

5 Usability-Evaluation des Videopasswort-Systems

Bereits im vorangehenden Pretest (siehe oben) konnte ein adäquates Bewertungsschema für die zeitlichen und räumlichen Abstände der Klicks identifiziert werden. Probanden trafen nur in Ausnahmefällen die korrekten 20x20-Pixel-Felder im Raster zum exakten Zeitpunkt. Dennoch zeigte sich in der Beobachtung der Probanden, dass diese nur in geringem Maße von der korrekten Setzung der Klickpunkte abwichen. Dadurch wurde deutlich, dass ein Bewertungsschema mit Gewichtungen erforderlich ist, das es ermöglicht, die Qualität der Anmeldungsversuche abzubilden. Dies ändert die Passwortprüfung von einem *exact match* in eine *Bewertungsfunktion*: werden Ort und Zeitpunkt der Klicksetzung nicht exakt getroffen, so berechnet das System eine Maßzahl für die Abweichung.
Es wird die These aufgestellt, dass ein Videopasswortsystem bei gleicher oder ähnlicher Usability eine höhere Sicherheit aufweist als vergleichbare Text- oder Bildauthentikationssysteme. Mit Hilfe einer benutzerzentrierten Evaluation sollten Erkenntnissen bezüglich der Usability, der Akzeptanz und der wahrgenommener Sicherheit gewonnen werden.

5.1 Testpersonen und Testablauf

Teilnehmer insgesamt	***127***		
Geschlecht		***IT-Erfahrung***	
Männlich	93	Sehr gut	42
Weiblich	34	Gut	47
Status / Ausbildung		Normal	34
Schuler, Student	72	gering	4
Berufstätig	51	***Alter***	
Sonstige	4	Durchschnitt	24,5 Jahre

Tabelle 1: Demografische Verteilung der Probanden.

Für die Überprüfung der Sicherheit der generierten Passwörter, der Akzeptanz des Verfahrens sowie Usability-Aspekten des Verfahrens wurden Benutzertests durchgeführt. Die demografische Verteilung der Teilnehmenden ist in Tabelle 1 dargestellt. Die Probanden sollten zunächst ein eigenes Videopasswort erstellen und dieses in einem zweiten Schritt zur Authentikation anwenden. Die Generierung eines individuellen Videopassworts erfolgte über

das Auswählen (Klick) von vier für den Benutzer markanten, d.h. memorierbaren Stellen im abspielenden Video.

Den genauen Ablauf des Nutzertests zeigt Abbildung 1. Durchgezogene Linien beschreiben Abschnitte mit zwingender Interaktion des Nutzers, Elemente aus gestrichelten Linien sind systemseitige Informationen ohne Nutzereingaben. Bei der Interaktion mit dem Videopasswortsystem werden Informationen über Ort und Zeitpunkt der Klickplatzierung gespeichert. Damit können zusätzlich zum Test des Systems auch Aussagen über die Sicherheit der gewählten Passwörter getroffen werden. Alle gewonnen Daten werden in einer Datenbank erfasst und mit Hilfe von Bewertungsschemata für die Dimensionen *Raum* und *Zeit* sowie Faktoren für einen erfolgreichen Login analysiert.

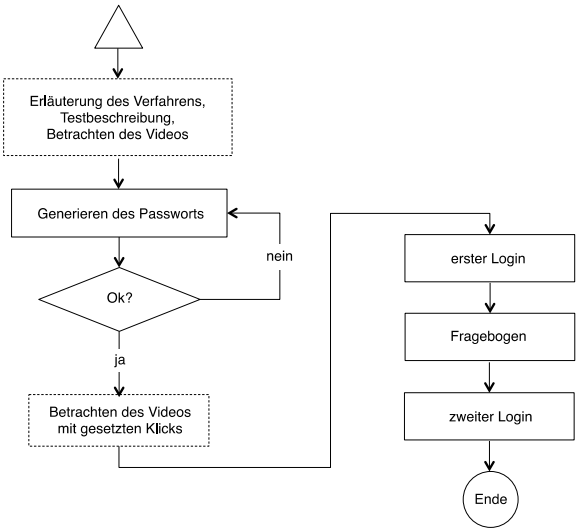

Abbildung 1: Ablauf des Nutzertests (Nutzerinteraktion aktiv und passiv).

5.2 Bewertungsschema

Da ein exakter Abgleich der Zuordnungen sich als schwierig herausgestellt hat, wurde ein Bewertungsschema entwickelt, das einen Wert der räumlichen und temporalen Nähe zur Vorgabe angibt:

Raum

In der räumlichen Auswertung wird überprüft, wie präzise die zuvor gesetzten Marken von den Nutzern getroffen wurden. Abbildung 2 zeigt das verwendete Bewertungsschema. Der grüne Bereich (Mitte) zeigt den Bereich einer gesetzten Marke an, der für eine erfolgreiche Identifikation getroffen werden musste. (20x20-Pixelraster, vgl. Abbildung 3 unten).

5	5	5	5	5	5	5	5	5	5	5
5	4	4	4	4	4	4	4	4	4	5
5	4	3	3	3	3	3	3	3	4	5
5	4	3	2	2	2	2	2	3	4	5
5	4	3	2	1	1	1	2	3	4	5
5	4	3	2	1	0	1	2	3	4	5
5	4	3	2	1	1	1	2	3	4	5
5	4	3	2	2	2	2	2	3	4	5
5	4	3	3	3	3	3	3	3	4	5
5	4	4	4	4	4	4	4	4	4	5
5	5	5	5	5	5	5	5	5	5	5

Abbildung 2: Bewertungsschema der Klicks im Raum.

Wurde die Marke beispielsweise auf das Feld *210* gesetzt und trifft der Nutzer beim Identifizierungsversuch das Feld *230*, ist dies eine Abweichung der Ursprungsmarkierung von 1 (grün) und liegt noch im Toleranzbereich (vgl. Abbildung 3).

Abbildung 3: Video-Raster.

Zeit

Die zeitliche Dimension wurde mit Hilfe des in Abbildung 4 dargestellten Schemas ausgewertet.

Differenz	-1,5	-1,2	-0,9	-0,6	-0,3	0	0,3	0,6	0,9	1,2	1,5
Grad	5	4	3	2	1	0	1	2	3	4	5

Abbildung 4: Bewertungsschema für die Klicks in der zeitlichen Dimension (in Sekunden).

Analog zur räumlichen Dimension wird ein geringer Toleranzbereich eingeräumt (grüne Felder). Anhand der Skala wird der Grad der Abweichung gemessen und bewertet. Weicht zum Beispiel der Zeitpunkt des Klicks maximal um 0,3 Sekunden von der gesetzten Marke ab, wird dieser mit *1* bewertet.

5.3 Erfolgskriterien (Bewertungsfunktion)

Die Bewertungsfunktion addiert räumliche und temporale Abweichungen anhand der oben dargestellten Bewertungstabellen auf. Für die Bestimmung der Erfolgsquote, also ob und wann sich ein Nutzer erfolgreich mit Hilfe des Videopassworts authentifizieren konnte, wurden folgende Kategorien festgelegt:

- *Problemlose Authentikation (Punkte im Bewertungsschema: 0-3)*

  Die Testperson konnte sich ohne Schwierigkeiten einloggen und hätte noch Spielraum für kleinere Abweichungen – zeitlich oder räumlich – gehabt.

- *Noch erfolgreiche Authentikation (Punkte im Bewertungsschema: 4-7)*

  Der Login war zwar erfolgreich, jedoch hat der Proband die gesetzten Grenzen weitestgehend ausgeschöpft.

- *Knapp fehlgeschlagene Authentikation (Punkte im Bewertungsschema: 8-11)*

  Durch eine minimale Überschreitung der zulässigen Abweichungen konnte sich der User nicht erfolgreich einloggen.

- *Erfolglose Authentikation (Punkte im Bewertungsschema: 12-15)*

  Grobe Abweichungen bei *Zeit und/oder Raum* verhindern einen validen Login.

- *Außerhalb des Bewertungsspektrums (Punkte im Bewertungsschema: >15)*

  Ein Login ist theoretisch unmöglich und fällt somit aus der Bewertung.

Unabhängig von möglichen Sicherheitsimplikationen dient die Kategorisierung des Authentikationserfolgs der besseren Bestimmung der Gebrauchstauglichkeit des Systems.

5.4 Auswertung

Die Evaluation erfolgte in mehreren Schritten. Zunächst wurde von den Benutzern ein eigens gewähltes Passwort generiert. Anschließend erfolgte die Evaluation der Usability anhand von zwei Login-Versuchen der Probanden. Folgende Fragen sollten dabei beantwortet werden:

- Wie hoch ist die Quote erfolgreicher Logins (Effektivität)?
- Ist ein Lerneffekt zwischen dem ersten und zweiten Authentikationsversuch zu erkennen?
- Wie hoch ist die Akzeptanz des Verfahrens bei den Probanden?

5.4.1 Erfolgsquote und Usability

Die Anzahl erfolgreicher Logins wurde neben dem Fragebogen als Maß zur Messung der Usability herangezogen. Es wird angenommen, dass eine höhere Erfolgsquote als Indikator für die Gebrauchstauglichkeit herangezogen werden kann. 92,1% der Probanden gaben an, dass *VidPass* einfach zu bedienen sei und die Bearbeitung der Aufgabenstellung keinerlei

Probleme bescherte. Die Auswertung der erfolgreichen Authentikation (in Bezug auf *Raum und Zeit)* ergibt im letzten Durchgang 67% - zwei Drittel der Probanden konnten sich also im Nutzertest mit dem zuvor unbekannten Authentikationsverfahren erfolgreich einloggen.

5.4.2 Lerneffekt

Es konnte ein deutlicher Lerneffekt bei den beiden Durchgängen festgestellt werden. Die Erfolgsquote steigerte sich von 57% im ersten Durchgang auf 67% positiver Authentikation im zweiten Durchgang. Dies lässt darauf schließen, dass zum einen Trainingseffekt bei der Verwendung stattgefunden hat und zum anderen, dass die vom Probanden selbst gesetzten Passwörter durch die Unterbrechung zum Ausfüllen des Fragebogens vom Ultrakurzzeitgedächtnis ins Kurzzeitgedächtnis übergehen konnten. Zusätzlich zeigte sich, dass sich das Verhältnis von „noch erfolgreicher Authentikation“ zu „problemloser Authentikation“ verbesserte – die Testpersonen wurden also genauer in ihren Eingaben.

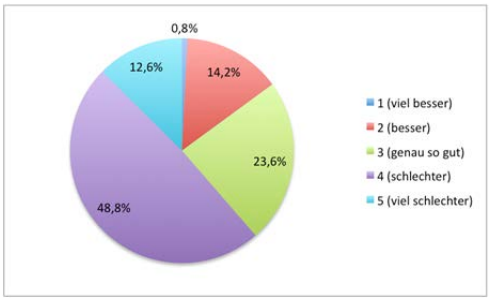

Abbildung 5: Benutzerakzeptanz von VidPass im Vergleich zu herkömmlichen Passwörtern.

5.4.3 Nutzerakzeptanz

Die Akzeptanz (Davis 1989) des Verfahrens wurde mit Hilfe eines Fragebogens erhoben. Im Vergleich mit herkömmlichen passwortbasierten Systemen hielten knapp 40% der Benutzer das Verfahren als „besser“ oder „genauso gut“ (Abbildung 5). Bei der Frage nach der Sinnhaftigkeit eines Einsatzes antworteten 45% der Nutzer, das Verfahren sei „sehr sinnvoll“ bis „einigermaßen sinnvoll“. 92% der Probanden gaben an, dass die Aufgabenstellung „sehr leicht“ oder „leicht“ verständlich war. Diese leichte Verständlichkeit lässt auf eine hohe Selbstbeschreibungsfähigkeit des Systems schließen. Die große Anzahl an Personen, die das Verfahren als Alternative für ein klassisches Passwortsystem in Betracht ziehen, zeigt die Relevanz für weitere Untersuchungen dieses Ansatzes.

5.4.4 Sicherheit

Die theoretische Entropie des Merkmalsraums, in dem sich Passwörter in *VidPass* erzeugen lassen, ist durch die Anzahl der Raster im Video sowie die zeitliche Segmentierung definiert. Im theoretischen Fall der Unabhängigkeit und gleichen Wahrscheinlichkeit der Klicksetzung ergibt sich als Shannon-Entropie des Systems in der vorliegenden Ausgestaltung ein Wert von 41,7 Bit. Bei der Betrachtung der tatsächlich aufgetretenen Klicks zeigt sich jedoch ein anderes Bild. Die Wahrscheinlichkeiten für die Setzung von Klicks ist stark abhängig von

der dargestellten Szene im Video. So ist deutlich wahrscheinlicher, dass ein markantes Element geklickt wird (beispielsweise ein Gesicht einer Hauptfigur beim ersten Auftreten), als ein zufälliges Feld in einer monotonen Fläche (etwa eines blauen Himmels). Dieser Faktor wird maßgeblich durch die Auswahl des Videoclips bestimmt. Durch die Einbeziehung eines Toleranzbereiches bei der Setzung von Klicks wird die Angabe zur tatsächlich aufgetretenen Entropie äußerst komplex und muss in weiteren Arbeiten genauer untersucht werden.

6 Diskussion und weiteres Vorgehen

Der Test eines Prototypen zur videobasierten Authentikation zeigt unterschiedliche Ergebnisse sowohl aus Sicht der Usability als auch der Akzeptanz und der Sicherheit. Einerseits gaben 90% der Testpersonen an, das System sei leicht zu benutzen. Andererseits schätzten weniger als die Hälfte das Verfahren als besser oder gleich gut im Vergleich zu herkömmlichen Passwörtern ein. Der Grund für die geringere Akzeptanz muss von anderen Faktoren abhängen. Zukünftige Untersuchungen sollen dieser Beobachtung nachgehen. Zudem lässt sich auf Basis der Ergebnisse vermuten, dass die Auswahl des Videoclips (vgl. Punkt 4) maßgeblichen Einfluss auf Benutzerfreundlichkeit und Nutzerakzeptanz zu haben scheint.

Die Betrachtung der Sicherheit des Verfahrens zeigt deutliche Unterschiede zwischen dem theoretisch möglichen Merkmalsraum und den tatsächlich aufgetretenen Klickpunkten. Angaben zur Sicherheit des Systems, speziell im Vergleich unterschiedlicher Videos, sind ein weiterer Aspekt für Folgestudien. Zu prüfen ist auch, inwiefern videobasierte Passworteingabe für bekannte Angriffsstrategien wie das *Shoulder Surfing* (Kumar et al. 2007) anfällig ist. Eine Koppelung mit alternativen Eingabetechniken, beispielsweise der blickbasierten Passworteingabe eröffnet zusätzliche Gestaltungsmöglichkeiten.

Eine abschließende Aussage über die Eignung und eventuelle Einsatzmöglichkeiten sowie generelle Verbesserungen des Verfahrens lassen sich in diesem frühen Stadium noch nicht treffen. Basierend auf den umfangreichen Aspekten, die ein erster Test eines Prototypen offenbart, kann das Verfahren als vielversprechender neuer Ansatz gesehen werden, der in vielen Disziplinen weitere Forschungsfragen liefert.

Literaturverzeichnis

Bauer, F. L. (2000). *Entschlüsselte Geheimnisse.* Berlin [u.a.]: Springer.

Biddle, R., Chiasson, S., van Oorschot, P. C. (2009). Graphical passwords: Learning from the first generation. *Technical Report TR-09-09,* Computer Science, Carleton University.

Chiasson, S., Forget, A., Biddle, R., & van Oorschot, P. C. (2008). *Influencing users towards better passwords: persuasive cued click-points*, S. 121-130.

Childers, T. L., & Houston, M. J. (1984). Conditions for a Picture-Superiority Effect on Consumer Memory. *The Journal of Consumer Research,* S. 643.

Davis, F. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information. In *MIS Quarterly. 13,*S. 319–340.

DeAngeli, A., Coventry, L., Johnson, G., & Renaud, K. (2005). Is a picture really worth a housand words? Exploring the feasibility of graphical authentication systems. *International Journal of Human-Computer Studies, 63(2005),* S. 128-152.

Federrath, H., Pfitzmann, A. (2006). IT-Sicherheit. In: Wind, M., Kröger, D. (Hrsg.). *Handbuch IT in der Verwaltung.* Heidelberg [u.a.]: Springer, S. 273-292.

Florencio, D. & Herley, C. (2007). A large-scale study of WWW password habits. In *16th ACM International World Wide Web Conference (WWW).*

Fox, D., Schäfer, F. (2009). Passwörter — fünf Mythen und fünf Versäumnisse. In: *Datenschutz und Datensicherheit - DuD, 33(7),* S. 425-429.

Hub, M., Čapek, J., Myšková, R., & Roudný, R. (2010). Usability versus security of authentication, In: *International Conference on Communication and Management in Technological Innovation and Academic Globalization (COMATIA '10).* Tenerife: WSEAS Press, 2010, S. 57-61.

Jansen, W., Gavrila, S., Korolev, V., Ayers, R., & Swanstrom, R. (2003). Picture password: A visual login technique for mobile devices. *Technical Report NISTIR 7030,* NIST.

Jermyn, I., Mayer, A., Monrose, F., Reiter, M., & Rubin, A. (1999). The design and analysis of graphical passwords. In *Proc. 8th USENIX Security Symposium.*

Kim-Phuong L. V., Proctor R.W., Bhargav-Spantzel, A., Tai B. (B.), Cook, J. & Schultz E. E. (2007). Improving password security and memorability to protect personal and organizational information. In: *International Journal of Human-Computer Studies 65(8) (2007),* S. 744-757.

Klingler, A. M. (2011). *Authentifizierungsverfahren und ihre Benutzerfreundlichkeit.* B.A.-Arbeit, CASED, TU Darmstadt, März 2011.

Kumar, M., Garfinkel, T. Boneh, D. & Winogard, T. (2007). Reducing shoulder-surfing by using gaze-based password entry. In *Proceedings of the 3rd symposium on Usable privacy and security.*

Maus, T. (2008). Das Passwort ist tot — lang lebe das Passwort! In: *Datenschutz und Datensicherheit - DuD, 32(8),* S. 537-542.

Moncur, W., & Leplâtre, G. (2007). Pictures at the ATM. In *Proceedings of the SIGCHI conference on Human factors in computing systems - CHI '07,* S. 887. New York, New York, USA: ACM Press.

Penninger, S., Meier, S., Federrath, H. (2012). Usability von CAPTCHA-Systemen. In *Sicherheit 2012. Sicherheit, Schutz und Zuverlässigkeit. Beiträge der 6. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), Lecture Notes in Informatics (P-195),* Michael Waidner, Suri Neeraj (Hrsg.), Köllen-Verlag, Bonn 2012, S. 199-208.

Sasse, M. A., Brostoff, S. & Weirich, D. (2001). Transforming the 'weakest link' – a human/computer interaction approach to usable and effective security. *BT Technology Journal, 19(3).* S. 122–131.

Singh, S. (2000). *Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet.* München [u.a.]: Hanser.

Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., & Memon, N. (2005). PassPoints: Design and longitudinal evaluation of a graphical password system. In *International Journal of Human-Computer Studies, 63(1-2),* S. 102-127.

Wood, C. C. Banks, W. W. Jr. (1993). Human error: an overlooked but significant information security problem. In *Computers & Security 12(1) (1993),* S. 51-60.