Passwords in general

Matthias Walthart
Diplom Wirtschaftsinformatiker
Technische Universität Darmstadt
walthart@rbg.informatik.tu-darmstadt.de

ACM CLASSIFICATION KEYWORDS
H.1.2 User/Machine Systems, Human Factors, Security

AUTHOR KEYWORDS
Usable security, Usability, Security, Authentication

EINLEITUNG

Für Informatiker ist ein Passwort eine größtenteils komplexe Verkettung von Zeichen, die zur Authentifikation verwendet wird. Für den Nutzer jedoch ist ein Passwort eine Last, denn es muss oft eingegeben werden und bei mehrfachen Falscheingaben droht die Verweigerung des entsprechenden Dienstes. Aber nicht nur diesem Problem sieht sich der Nutzer ausgesetzt, bei einer Vielzahl an Diensten erhöht sich ebenso die Anzahl der zu merkenden Passwörter, was viele Nutzer schlichtweg überfordert. In gerade solchen Situationen der Überforderung der Nutzer durch zu viele oder zu komplizierte Passwörter, sind diese dazu geneigt, durch aufschreiben oder das mehrfache Verwenden ihrer Passwörter, die aufgestellten Passwort-Richtlinien zu umgehen[11].

Diese Seminararbeit befasst sich mit dem Dilemma der Passworte: „**Sicherheit oder Benutzbarkeit**“[7] und soll einen Überblick über die aktuellen Hilfsmittel zur Lösung dieses Dilemmas geben. Hierbei stellt sich anfangs die Frage, ob ein komplexeres Passwort auch gleichzeitig zu mehr Sicherheit führt, da davon ausgegangen werden kann, dass Passwörter ab einem gewissen Komplexitätslevel nicht mehr gemerkt, sondern irgendwo aufgeschrieben werden. Es ist sicher nicht im Sinne der hochmodernen und sicheren IT-Dienste, wenn deren Passworte per Notizzettel an den Bildschirmen kleben.

Dem Nutzer kann aber geholfen werden. Es gibt viele Methoden und Hilfsmittel, die es ermöglichen auch mit einer Vielzahl von komplexen Passwörtern umzugehen, ohne den Überblick zu verlieren oder die Sicherheits-Richtlinien zu unterlaufen. Hierbei gibt es die unterschiedlichsten Ansätze. Das Spektrum reicht von Methoden, die dem Nutzer das bessere Erinnern an seine Passwörter ermöglichen sollen bis zu technischen Hilfsmitteln, die ihm die gesamte Passwortverwaltung abnehmen können. Bei letzteren Hilfsmitteln ist es dann oft nur noch nötig, sich ein einziges Passwort zu merken.

In dieser Seminararbeit werden erst einmal die Grundlagen für eine Definition von Sicherheit dargelegt um darauf aufbauend die gängigsten und vielversprechendsten Methoden und Hilfsmittel für Nutzer vorzustellen, sowie die Verbreitung und den Mehrwert dieser Tools für den Nutzer aufzudecken und zu belegen. Abschließend wird ein Ausblick auf die zukünftigen Entwicklungen gegeben und die Chance bewertet, ob textuelle Passwörter durch Alternativen abgelöst werden könnten.

GRUNDLAGEN

Das folgende Kapitel erläutert zunächst die Grundlagen für die weiteren Ausführungen. Es wird im Speziellen auf die Sicherheitsmaßstäbe eingegangen, an denen Passwörter in dieser Arbeit gemessen werden. Weiterhin wird dargestellt, wie groß die Problematik im Umgang mit Passwörtern ist und welche Alternativen zur Verfügung stehen.

Sicherheitsanforderungen für Passwörter

In dieser Arbeit wird der Sicherheit von Passwörtern ein einheitliches Angriffsszenario zugrunde gelegt. Dabei besitzt der Angreifer die Möglichkeit, für einen Nutzernamen Passwörter seiner Wahl zu testen bis er das korrekte Passwort gefunden hat. In der Realität sind solche Angriffe meist mit einer limitierten Anzahl von Versuchen oder hohem zeitlichen Aufwand verbunden[1]. Dennoch ist dieses Szenario sehr gängig für eine Sicherheitsbetrachtung von Passwörtern, da es genügend Situationen gibt, in denen der Angreifer **direkten Zugriff zu der Passwortdatei** erlangen kann, wo das Passwort in seiner gehashten Form abgespeichert ist:

- Der Angreifer ist gleichzeitig Administrator des Systems und kann jederzeit auf diese Datei zugreifen (sog. „Angriff von Innen“).
- Der Angreifer dringt durch eine Sicherheitslücke in das System ein und schafft es die Datei auszulesen.
- Der Angreifer belauscht die Kommunikation eines Nutzers mit dem System in der das Passwort in gehashter Form übertragen wurde.

[1] Die Zeit zwischen zwei Versuchen steigt kontinuierlich mit der Anzahl der Versuche. Auch ist eine feste Limitierung der Versuche üblich (z.B. bei PINs von Mobiltelefonen und Bankkarten).

Auf diese Dateien kann der Angreifer dann mit geeigneten Tools einen Brute-Force- oder auch Wörterbuchangriff durchführen. Beim Brute-Force-Angriff werden lediglich alle möglichen Buchstaben-Kombinationen ausprobiert (dauert in der Regel sehr lange), während beim Wörterbuchangriff eine Liste mit gängigen Passwörtern durchprobiert wird (nimmt vergleichsweise weniger Zeit in Anspruch, findet aber nicht jedes Passwort).

Tools wie „John the Ripper“[8] oder „Passwortcracker“ können je nach Rechner ca. 200.000 Passwörter pro Sekunde testen. Aus der Komplexität eines Passworts und seiner Länge lässt sich also die maximale Zeit errechnen, die ein solches Tool für das Herausfinden benötigt (siehe Tabelle 1).

Qualität	**Passwortlänge**		
	6	**8**	**10**
bekanntes Wort	< 1 Sekunde		
Wortähnlich	< 30 Sekunden		
A-Z	13 Min.	6 Tage	11 Jahre
A-Z,a-z	14 Std.	4 Jahre	11.500 Jahre
A-Z,a-z,0-9, Sonder	6 Tage	98 Jahre	580.800 Jahre

Tabelle 1: Maximaler Zeitaufwand eines Angriffs

In Unternehmen besagen Passwortrichtlinien meist, dass sämtliche Passwörter regelmäßig geändert werden müssen. Dabei werden Zeiträume von ca. 3-6 Monaten vorgegeben, in denen ein Passwort gültig bleibt. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) schlägt ähnliche Maßnahmen vor. Es empfiehlt mindestens 8 Zeichen, Groß-/Kleinschreibung, Zahlen, Sonderzeichen und keine bekannten Wörter zu verwenden, sowie einen Turnus von 6 Monaten für den Wechsel des Passworts. Für ein wie oben beschriebenes Angriffs-Szenario empfiehlt das BSI sogar eine Passwortlänge von 20 Zeichen (z.B. für WLAN-Schlüssel)[10].

Aus einem solchen Zeitfenster kann nun die Sicherheitsanforderung für ein sicheres Passwort im oben genannten Szenario abgeleitet werden:

sicher
Das Passwort widersteht einem Brute-Force- oder Wörterbuchangriff im Durchschnitt mindestens 2 Jahre. Darunter fallen alle Passwörter, die nicht in Wörterbüchern stehen, mindestens 10 Zeichen haben, sowie Passwörter mit Groß - und Kleinschreibung (oder komplexer), die mindestens 8 Zeichen haben.

anfällig
Das Passwort widersteht einem Brute-Force- oder Wörterbuchangriff im Durchschnitt nicht länger als 6 Monate. Dazu zählen Passwörter, die nur 6 Zeichen haben oder nur aus Großbuchstaben bestehen und maximal 8 Zeichen lang sind.

unsicher
Das Passwort widersteht einem Brute-Force- oder Wörterbuchangriff im Durchschnitt nicht länger als einige Stunden. Dies trifft auf alle Passwörter zu, die in einem Wörterbuch stehen bzw. aus einem solchen abgeleitet werden können.

Diese Definitionen werden im Folgenden als Maßstab für die Sicherheit eines gewählten Passwortes herangezogen.

Bedeutsamkeit des Themas
Aktuelle Studien gibt es zu den verschiedensten Themen, so auch zur Benutzbarkeit von Passwörtern. In Artikeln wie „Passwörter überfordern Mitarbeiter"[4] und „Leichtsinn bei Passwörtern ermöglicht Datenklau"[9] wird immer wieder auf die Probleme und Risiken beim Umgang mit Passwörtern hingewiesen. Auch wissenschaftliche Arbeiten befassen sich mit diesem Thema. Alle kommen aber zu dem gleichen Ergebnis: Das Problem ist nicht das Passwort selbst, sondern der Mensch, der es benutzt.

Studien zeigen, dass 40 % der Nutzer ihr Passwort an andere (z.B. Kollegen) weitergeben und **55 % haben ihr Passwort irgendwo notiert**[16]. Gerade eine Weitergabe des Passwortes hebelt jegliche Authentifikation aus, denn ist das eigene Passwort erst einmal weitergegeben, ist eine eindeutige Zuweisung von Person zu Zugangsdaten nicht mehr möglich[1,17].

Letztendlich führt daher kein Weg daran vorbei, den Nutzer selbst auf die Wichtigkeit der Passwortsicherheit aufmerksam zu machen. In manchen Sicherheits-Konzepten wird genau dies vorgeschlagen, denn erst wenn ein Nutzer einmal selbst in der Situation gewesen ist, dass sein Passwort geknackt wurde, geht er sorgsamer mit seinen Passworten um. Um diese Situation gar nicht erst aufkommen zu lassen, kann den Nutzern demonstriert werden, was die aktuellen Möglichkeiten der Passwortknacker sind. Vor allem der zeitlichen Aufwand für aktuelle Angriffsverfahren wird von vielen Nutzer meist kolossal unterschätzt[2,15].

Alternativen zu Passwörtern
Es wäre alles einfacher, wenn man Passwörter durch ein neues System ablösen könnte. Doch welches System sollte dafür gewählt werden? In Diskussionen zu diesem Thema fallen immer wieder die gleichen Begriffe:

- Biometrie
  Der Fingerabdruck ersetzt das Text-Passwort.

- Graphische Passwörter
  Das Passwort besteht nicht mehr aus Textzeichen sondern aus Bildpunkten oder Icons.
- One-Time-Passwörter (z.B. mit Mobiltelefonen)
  Bei jeder Authentifikation bekommt der Nutzer ein neu generiertes Passwort geschickt.
- PKI[2] (z.B. mit Smartcards)
  Ein digitales Zertifikat dient als Basis der Authentifikation.
- Psylock[3]
  Das spezifische Tippverhalten des Nutzers wird für die Authentifikation verwendet.

Doch all diese Verfahren sind nur bedingt geeignet um das Sicherheitssystem „Passwort" abzulösen. Biometrie, Smartcards und One-Time-Passwörter benötigen spezielle Zusatzgeräte, wie Kartenleser oder das Mobiltelefon. Auch die graphischen Passwörter sind nur eingeschränkt nutzbar, denn sie benötigen in der Regel ein relativ hochauflösendes Display und eine Maus. Diese zusätzlichen Hilfsmittel stehen aber nicht in allen Situationen zur Verfügung und deshalb muss immer wieder auf textuelle Passwörter zurückgegriffen werden.

Bei vielen Diensten lohn sich auch schlicht weg der Einsatz von vergleichsweise teuren Biometrie- oder PKI-Verfahren nicht. Für ein einfaches Forum würde ein solcher Sicherheitsmechanismus überzogen sein. Bei einem Bankaccount, bei dem es direkt um Geld geht, das bei unbefugten Zugriff in Gefahr gerät, wären solche Verfahren schon eher lohnenswert.

HAUPTTEIL

Dieser Teil der Seminararbeit geht auf die Probleme und Lösungsversuche in Bezug auf Passwörter ein. Es werden sowohl Sicherheit als auch Benutzerfreundlichkeit bewertet, sowie einen Überblick über die aktuellen Entwicklungen gegeben.

Probleme mit Passwörtern

Textuelle Passwörter bringen eine Reihe von Problemen mit sich. Doch erst die aktuellen Entwicklungen sowohl auf dem Gebiet der Sicherheitstechnik, als auch auf dem Gebiet des Computerbaus haben diese Probleme an einen Punkt gebracht, an dem über Lösungen und Alternativen aktiv nachgedacht werden muss.

Die größten Probleme sind derzeit:

1. Passwörter werden immer komplexer.
2. Passwörter werden immer länger.
3. Die Anzahl der Passwörter nimmt immer mehr zu.

Der Ursprung dieser Probleme ist zwar nicht der Nutzer selbst, aber er ist es, der mit den Sicherheitsanforderungen einfach überfordert wird, denn Passwörter sind für ihn nicht mehr merkbar und er sucht nach Abhilfen, die wiederum neue Probleme aufwerfen[1,13]:

1. Passwörter werden möglichst einfach gewählt.
2. Passwörter werden beim vorgeschriebenen Wechseln nur wenig oder leicht nachvollziehbar abgeändert.
3. Passwörter werden aufgeschrieben.
4. Passwörter werden weitergegeben.
5. Passwörter werden mehrfach verwendet.

Da sich die 3 Ursprungsprobleme nur schwer lösen lassen, wird versucht, die Probleme der Nutzer mit Methoden zur Gedächtnisverbesserung, Tools zur Passwortbewertung und ganzen Passwortverwaltungen zu lösen. Welche davon das Richtige für einen speziellen Nutzer sind, muss der Nutzer allerdings selbst entscheiden, da nicht alle Hilfsmittel ihm gleichsam nützlich sind[5].

Hilfen für den Nutzer

Um dem Nutzer die Wahl und Verwaltung seiner Passwörter zu erleichtern gibt es verschiedene Typen von Hilfsmitteln. Alle haben jedoch ein gemeinsames Ziel: Dem Nutzer soll geholfen werden, seine Probleme mit Passwörtern zu lösen, damit er trotz Menge oder Komplexität der Passwörter geltende Passwort-Richtlinien einhalten kann.

Methoden

Da sich Nutzer ihre komplexen Passworte schlecht merken können, gibt es Methoden um genau dieses Problem zu lösen. Ein Beispiel ist, dass **einfache Sätze** genommen werden, um sie in Passwörter umzuformen, denn solch ein Satz kann sich leichter gemerkt werden als ein komplexes (und damit sicheres) Passwort[14,18].

Der Nutzer muss sich für sein sicheres Passwort also erstmal einen beliebigen Satz ausdenken und sich diesen merken. Mit ein paar einfachen Transformationsregeln kann er dann im zweiten Schritt daraus sein Passwort ableiten. Aus dem Satz „Alas, poor Yorick! I knew him, Horatio" aus Shakespeares' „Hamlet" entsteht dann das Passwort „A,pY!Ikh,H". Ein solcher Satz lässt sich aus beliebigen Büchern, Hobbys oder persönlichen Erfahrungen bilden. Auch das BSI empfiehlt dieses Vorgehen bei der Passwortwahl[10].

Mit dieser Methode werden gleichzeitig die beiden größten Probleme der Nutzer gelöst:

1. Was ist ein sicheres Passwort?

[2] Eine Public Key Infrastruktur (PKI) besteht aus einem System von digitalen Zertifikaten die zur Authentifikation diehnen und auf Smartcards gespeichert werden können.

2. Wie merke ich mir dieses Passwort?

Auf diese Weise generierte Passwörter sind zwar relativ sicher gegen die heutigen Angriffsmethoden, aber da die Sätze meist im Internet auffindbar sind (und somit öffentlich), könnte ein Wörterbuch speziell für diese Passwörter erstellt werden, welches eine Angriffsanfälligkeit stark erhöhen könnte. Zurzeit existieren solche Wörterbücher aber noch nicht. Des weiteren ist diese Methode nicht generell geeignet ein sicheres Passwort zu erzeugen, da einfache Sätze auch zu vergleichsweise unsicheren Passwörtern führen.

Dieses Verfahren löst somit zumindest für wichtige Passwörter das „Merk-Problem“, aber bei immer mehr Diensten oder Passwörtern stößt ein Nutzer auch schnell wieder an seine geistigen Grenzen. Um außerdem sicher zu gehen, dass ein sicheres Passwort erzeugt wurde, sollte das neue Passwort anschließend durch ein Test-Tool auf seine Sicherheit geprüft werden.

Tools zur Passwortbewertung

Um den Nutzern das Wählen eines neuen Passwortes zu erleichtern, gibt es Assistenten, die die Stärke eines Passwortes bewerten können (Abbildung 1). Im Gegensatz zu den zuvor beschriebenen Methoden wird das Augenmerk hier ausschließlich auf die Stärke des Passwortes gelegt. Die Möglichkeit sich das sichere Passwort gut merken zu können wird nicht betrachtet.

Abbildung 1: Passwort-Check von CrypTool-Online.org

Ein solcher Passwort-Assistent untersucht das Passwort nach verschiedenen Kriterien für sichere Passwörter, von denen auch schon die Wichtigsten im Kapitel „Sicherheitsanforderungen für Passwörter“ vorgestellt wurden. In der Regel werden die Komplexität und die Länge des gewählten Passwortes bewertet. Die besseren Passwort-Assistenten betrachten darüber hinaus noch die Anfälligkeit für bestimmte Angriffsmethoden, wie z.B. Wörterbuchangriffe. Am weitesten verbreitet sind aber immer noch die Assistenten, die **eine rein theoretische Betrachtung** durchführen. Vor allem, weil sie schneller Ergebnisse liefern und sich meist in den Bewertungen nicht von denen besseren Assistenten unterscheiden[6].

Aus dem Internet sind solche Assistenten nicht mehr weg zu denken, da sie regelmäßig bei Foren als Hilfsmittel für die Passwortvergabe während der Registrierung Verwendung finden.

Tools zum Passwortmanagement

Noch weiter als eine reine Bewertung gehen die Tools, die die komplette Passwortverwaltung übernehmen können (Abbildung 2). In diesem Fall muss sich der Nutzer lediglich ein Passwort merken und nicht mehr sämtliche Passwörter für alle seine Zugänge. Dieses **Master-Passwort** sollte aber ein sicheres Passwort sein, da bei Bekanntwerden des selbigen gleich alle Passwörter kompromittiert würden. Für den Nutzer ist das Master-Passwort aber ein Segen, denn er muss sich nun nur noch dieses einzige Passwort merken und wird auch nicht gezwungen es regelmäßig zu ändern. Bei den Passwortverwaltungen, die in den aktuellen Browsern wie Firefox oder Internet Explorer mitgeliefert werden, ist sogar gar kein Master-Passwort mehr erforderlich[3].

Es gibt viele solcher Passwortverwaltungstools und alle haben die Basisfunktion Passwörter zu speichern. Manche haben darüber hinaus jedoch noch weitere nützliche Funktionen.

Ein Beispiel für eine extra Funktion liefert „Passpet“, eine Passwortverwaltung mit **Phishing-Schutz**. Diese Passwortverwaltung speichert nicht nur das Passwort, sondern schützt auch den Nutzer vor der unbeabsichtigten Eingabe des Passworts auf einer von Angreifern präparierten Webseite (Phishing). Passpet zeigt ein kleines Symbol neben der Adressleiste des Browsers, um die Echtheit der Webseite anzuzeigen und damit vor einem solchen Phishing-Angriff zu schützen[19].

Die Passwortverwaltung „Password Multiplier“ verwaltet nicht nur Passwörter, es generiert sie auch selbst. Aus dem Master-Passwort und einer Site-ID (meist der Webseitenadresse) wird das Passwort für diese Webseite generiert und in die Loginformulare eingetragen (siehe Abbildung 2). Aber die automatische Generierung hat auch Nachteile: Bei einem Passwortwechsel muss eine neue Site-ID gewählt werden, die dann nicht mehr so einfach merkbar ist. Gerade bei häufigen Passwortänderungen kommt hier auf den Nutzer wieder das Problem zu, dass er sich pro Passwort etwas zusätzlich merken muss. Wenigstens ist die Site-ID keine geheime Information wie das Master-Passwort und lässt sich deshalb relativ gefahrlos notieren[5,12].

[3] Passwortverwaltungen ohne Master-Passwörter bergen aber zusätzliche Sicherheitsrisiken.

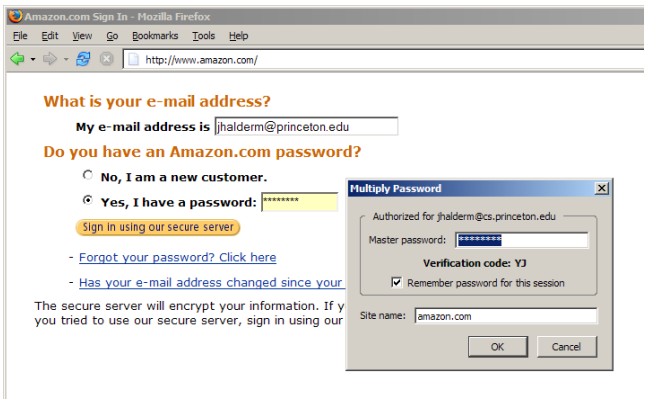

Abbildung 2: Passwortverwaltung mit Password Multiplier

In Bezug auf die Verwendbarkeit gibt es aber auch bei den Passwortverwaltungen Einschränkungen:

- Der Nutzer muss sich ein komplexes Passwort für den Zugriff auf die Passwortverwaltung merken.
- Der Nutzer kann nur von seinem Rechner auf geschützte Dienste zugreifen.
- Viele Dienste haben zusätzliche Sicherungen, so dass ein gespeichertes/verwaltetes Passwort nicht zur vollständigen Authentifikation ausreicht.
- Es lassen sich nicht immer alle Passworte mit diesen Hilfsmitteln verwalten (in der Regel keine Unterstützung für das Windows-Login-Kennwort und Passwörter von lokalen Applikationen).

Bei den vorgestellten Vorteilen dieser Passwortverwaltungen darf aber auch ein neu hinzukommendes Risiko nicht vergessen werden. Das Master-Passwort für die Passwortverwaltung könnte geknackt werden und ein Angreifer könnte damit alle Passwörter für sämtliche Dienste in Erfahrung bringen. Zugegeben, der Angreifer braucht dazu eine direkte Kontrolle des Rechners des Nutzers, aber dies war auch schon Bestandteil der Sicherheitsszenarien aus der anfangs getroffenen Definition von Sicherheit. Leider erfährt man auch aus aktuellen Berichten nur allzu oft, dass Rechner von Angreifern kontrolliert werden konnten, was bei einem geknackten Master-Passwort fatal wäre.

Letztendlich ist eine Passwortverwaltung mit einem sicheren Master-Passwort aber ein guter Kompromiss zwischen Sicherheit und Benutzbarkeit. Falls das Master-Passwort dann noch aus einem Satz abgeleitet und durch ein Test-Tool geprüft wurde, ist der Nutzer gut gegen die gängigsten Angriffsversuche abgesichert.

Die aktuellen Entwicklungen

Bei der Diskussion um Passwörter gibt es verschiedene Sichtweisen, die abhängig davon sind, ob eher eine Lösung auf Seiten der Nutzer oder der Sicherheitsarchitekturen präferiert wird. Einerseits kann man dem Nutzer Hilfsmittel und Methoden an die Hand geben sich auch komplexe Passwörter merken zu können, andererseits könnten aber auch die zu sichernden Dienste mit alternativen Authentifizierungsmethoden ausgestattet werden. Die zentrale Frage hierbei lautet also: Kann dem Nutzer ein ausreichend komplexes Passwort noch zugemutet werden, oder ist ein solcher Versuch von Vornherein zum Scheitern verurteilt, so dass auf andere Methoden ausgewichen werden muss?

Passwort-Richtlinien für die Nutzer

Im Falle eines komplexen Passwortes stellt sich die Frage nach der Durchsetzbarkeit, d.h. ob ein Nutzer eine Richtlinie für ein komplexes Passwort überhaupt befolgen wird. Denn wenn er eine Möglichkeit sieht bzw. bekommt die Richtlinie zu umgehen, wird er sie nutzen[17]. Gerade hier ist mit Richtlinien nur schwer eine Lösung zu erzielen, so dass einige Lösungsvorschläge eher auf Aufklärung als auf einen solchen Zwang setzen, wobei die Meinungen über den richtigen Weg stark auseinander gehen. Glaubt man den Befürwortern der Aufklärung, so wird der Nutzer immer einen Weg finden, die gesetzten Passwort-Richtlinien umgehen zu können. Die Befürworter des Zwangs halten indes dagegen, dass den Nutzern das technische Verständnis fehle, um die Notwendigkeit der Geheimhaltung und Sicherheit von Passworten überhaupt begreifen zu können.

Zusammenfassend lässt sich sagen, dass die Passwort-Richtlinien immer mehr auf Aufklärung und ein angebrachtes Komplexitätslevel setzen werden, da das **Dilemma für den Nutzer erkannt** wurde[2].

Technische Maßnahmen

Es ist leicht feststellbar, dass auf der technische Seite kräftig weiterentwickelt wird. Einerseits werden wegen aktueller und zukünftiger Sicherheitsrisiken wichtige Dienste, wie Bankaccounts, durch alternative oder zusätzliche Mechanismen geschützt, andererseits werden die Passwort-Alternativen weiter verbessert, so dass diese immer mehr die **Text-Passwörter ablösen** können.

Gerade bei den sehr wichtigen Diensten wie einem Bankaccount oder auch dem Zugang ins firmeneigene Netzwerk wird häufig nicht mehr auf reine Passwörter zurückgegriffen. Hier wird meist Gebrauch von PKI oder persönlichen Sicherheitstokens für One-Time-Passwörter gemacht. Bei den nicht so wichtigen Diensten wie sozialen Netzwerken oder Foren sind Passwörter aber nicht weg zu denken. Hier besteht das größte Potential für Alternativen wie graphischen Passwörtern den textuellen Login abzulösen.

FAZIT

Es gibt viele Nutzer, die aus den verschiedensten Gründen die Sicherheit ihrer Passwörter durch aufschreiben,

mehrfach verwenden oder weitergeben aufs Spiel setzen. Dabei existieren genügend Hilfsmittel für einen Nutzer seiner Passwörter Herr zu werden, ohne dabei gleichzeitig die Sicherheits-Richtlinien unterlaufen zu müssen. Allerdings werden diese Hilfsmittel nicht so häufig eingesetzt, wie es sich die Sicherheitsexperten dieser Welt wünschten, sei es durch Unwissenheit, oder weil der Anwendungsbereich der Hilfsmittel einfach zu klein ist. Nichtsdestotrotz ist man sich heutzutage dieser Problematik bewusst und es wird an immer besseren Hilfsmitteln gearbeitet.

Zukünftig wird das textbasierte Passwort wohl immer mehr aus unserem Alltag verschwinden, da es mehr und mehr durch neuere Methoden abgelöst wird, die entweder besser auf die Sicherheitsanforderungen (PKI, OTP) oder die Nutzerbedürfnisse (graphische Passwörter, Tippverhalten) abgestimmt sind.

LITERATUR

1. A. Adams and M. A. Sasse. Users are not the enemy. *Commun. ACM*, 42:40–46, December 1999.
2. H. Baier and T. Straub. Awareness by doing - ein neues konzept zur sensibilisierung von it-anwendern., 2005. http://www.informatik.tu-darmstadt.de/GK/staff/straub/publications/straub_awareness_2005.pdf.
3. D. Bartmann and M. Wimmer. Kein problem mehr mit vergessenen passwörtern. *Datenschutz und Datensicherheit - DuD*, 3:199–202, 2007.
4. I. Butters. Passwörter überfordern mitarbeiter, 2005. http://www.cio.de/_misc/article/printoverview/index.cfm?pid=153&pk=808539&op=pdf.
5. S. Chiasson, P. C. V. Oorschot, and R. Biddle. A usability study and critique of two password managers. In *In Proceedings of the 15th USENIX Security Symposium*, pages 1–16, 2006. http://www.usenix.org/event/sec06/tech/full_papers/chiasson/chiasson.pdf.
6. R. M. Conlan and P. Tarasewich. Improving the Password Selection Mechanism.
7. S. Fischer-H¨ubner, L. L. Iacono, and S. M¨oller. Usable security and privacy. *Datenschutz und Datensicherheit - DuD*, 11:773–782, 2010.
8. A. Forget, S. Chiasson, P. C. van Oorschot, and R. Biddle. Improving text passwords through persuasion. In *Proceedings of the 4th symposium on Usable privacy and security*, SOUPS '08, pages 1–12, New York, NY, USA, 2008. ACM.
9. D. Friedrich. Leichtsinn bei passwörtern ermöglicht datenklau, 2005. http://www.cio.de/_misc/article/printoverview/index.cfm?pid=158&pk=811589&op=pdf.
10. B. für Sicherheit in der Informationstechnik. Passwörter. https://www.bsi-fuer-buerger.de/cln_030/BSIFB/DE/ITSicherheit/SchuetzenAberWie/Passwoerter/passwoerter_node.html.
11. S. Gaw and E. W. Felten. Password management strategies for online accounts. In *Proceedings of the second symposium on Usable privacy and security*, SOUPS '06, pages 44–55, New York, NY, USA, 2006. ACM.
12. J. A. Halderman, B. Waters, and E. W. Felten. A convenient method for securely managing passwords. In *Proceedings of the 14th international conference on World Wide Web*, WWW '05, pages 471–479, New York, NY, USA, 2005. ACM.
13. B. Ives, K. R. Walsh, and H. Schneider. The domino effect of password reuse. *Commun. ACM*, 47:75–78, April 2004.
14. C. Kuo, S. Romanosky, and L. F. Cranor. Human selection of mnemonic phrase-based passwords. In *Proceedings of the second symposium on Usable privacy and security*, SOUPS '06, pages 67–78, New York, NY, USA, 2006. ACM.
15. M. A. Sasse, S. Brostoff, and D. Weirich. Transforming the 'weakest link' - a human/computer interaction approach to usable and effective security. *BT Technology Journal*, 19:122–131, July 2001.
16. R. Shay, S. Komanduri, P. G. Kelley, P. G. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor. Encountering stronger password requirements: user attitudes and behaviors. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, pages 2:1–2:20, New York, NY, USA, 2010. ACM.
17. T. Straub. *Usability Challenges of PKI*. PhD thesis, TU Darmstadt, Darmstadt, April 2006.
18. J. Yan, A. Blackwell, R. Anderson, and A. Grant. The memorability and security of passwords – some empirical results. Technical report, 2000.
19. K.-P. Yee and K. Sitaker. Passpet: convenient password management and phishing protection. In *Proceedings of the second symposium on Usable privacy and security*, SOUPS '06, pages 32–43, New York, NY,USA, 2006. ACM.