Passwords – Are You Current and Secure?
Contents
Why Do We Dislike Passwords? .......................................................... 3
Do We Need Passwords? ................................................................. 4
Current Practice .............................................................................. 5
  Password Security Standards ......................................................... 5
  Password Management ................................................................. 7
  Complexity and Cracking ............................................................... 8
Factors to Consider When Evaluating Password Policy .......................... 9
About Kevin P. Martin & Associates ................................................ 10
Works Cited ..................................................................................... 10
Why Do We Dislike Passwords?

Because they are complicated and hard to remember, right?

In December of 2012, a psychology research paper was published by a group of researchers at the Pontifical Catholic University of Rio Grande do Sul, Brazil. The research involved a survey to identify the practices of passwords usage as focused on memory limitations due to age and education backgrounds of users. During interviews of 263 individuals (150 female, 113 male), the team probed for information on participants’ current password use: what the passwords were used for, how many characters were used and the complexity standards, whether passwords were chosen or automatically assigned, and what type of information the password contained, such as birthdays, account numbers, or anniversaries.

The team expected to see a correlation between the user’s age and difficulty/forgetfulness when it came to memorization of passwords; but instead they found the biggest influence on memory performance was the number of instances in which the user has to use passwords. Simply put, the more passwords you have to memorize, the more you are going to mix them up or forget them.

Of the 1415 unique passwords studied, the research team discovered that the majority were numeric only (62.6%) and less than 1% (actual 0.7%) contained what most people would consider a “secure” password with a combination of numbers, letters, and special characters. It was also noted that 70% of all the passwords were user created instead of system generated. These results seem to support the current desire for better password security enforcement that meet standards and comes with less hassle for the user.

Prior research into information systems passwords revealed that people use rather insecure (and inappropriate) practices when choosing passwords simply because this makes them easier to remember. The more sensitive the data being protected, usually the more frequently users are forced to change the password. They found that the difficulty in recalling a password is not significantly related to its length. Also, choosing an easy to remember password does not stop users from writing it down. Even with rigorous training procedures, users can still persist in maintaining bad password habits. Perhaps some of this is sounding familiar?

1 Source: http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0051067
2 Source: http://www.rmu.edu/SentryHTML/pdf/lib_finn_DISCR710_password_security.pdf
3 Source: http://www.rmu.edu/SentryHTML/pdf/lib_finn_DISCR710_password_security.pdf
4 Source: http://www.hfes.org/web/newsroom/hfes09-foonaker-cis.pdf
Do We Need Passwords?

According to Petition Against Passwords, an advocacy campaign comprised of high-tech companies based in the Silicon Valley, we don't. Petition Against Passwords would prefer that we do away with little enforced policies and password complexity requirements in favor of what is called “passwordless” authentication.5

On the current cutting edge of technology we could even do away with passwords altogether and opt for a tattoo for authentication. The tattoo has already been developed by MC10, a Massachusetts-based engineering company, and involves the placement of a “stamp” on the skin containing flexible circuitry. A user can merely place a smartphone near the tattoo for verification purposes. Motorola is interested in using this technology as well as the Proteus Digital Health Pill, which generates a signal when ingested that could be recognized by the user's smartphone.6

Two-Factor authentication (also referred to as multi-factor authentication) is a type of authentication based on something you have and something you know. It is a means by which to decrease the probability that someone else is trying to access your account. Two-factor authentication involves at least two of three authentication factors, which are the categories by which someone may be authenticated or identified:7

1. Ownership factors – these represent something the user has in their possession. Examples are an ID card, security token, or mobile phone.
2. Knowledge factors – this is something that the user knows, such as a password, pass phrase, or personal identification number (PIN).
3. Inherence factors – this is something that the user is or does. Examples include biometric identifiers such as fingerprints, retinal pattern, voice or facial recognition.

6 Source: [http://www.dailytech.com/Motorola+Wants+to+Use+Tattoos+Pills+Instead+of+Smartphone+Passwords/article31671.htm](http://www.dailytech.com/Motorola+Wants+to+Use+Tattoos+Pills+Instead+of+Smartphone+Passwords/article31671.htm)
7 Source: [https://en.wikipedia.org/wiki/Authentication](https://en.wikipedia.org/wiki/Authentication)
Examples of using two-factor authentication can include:

- Inserting a bank card (ownership factor) and providing a PIN number (knowledge factor) at an ATM.
- Accessing a business network by providing a password (knowledge factor) and a number from a security token (ownership factor).
- Access to a high-security system via fingerprint check (inherence factor) and a PIN code (knowledge factor).
- Accessing online bank account with User Id and Password (knowledge) and then another Password that the bank system has messaged via text to your smartphone (ownership factor).

Until these new emerging technologies fully develop we need to accept the fact that we are all dependent on some form of password use for authentication. Therefore our goal should be to adopt realistic password controls that are “memorable” while still adhering to acceptable standards and practices.

**Current Practice**

**Password Security Standards**

There are a number of security standards that can be referenced when determining the most password strength for your company:

- The United States Government Configuration Baseline (USGCB)
- Federal Desktop Core Configuration (FDCC) – recommended by the National Institute of Standards and Technology (NIST)
- Payment Card Industry Data Security Standards (PCI-DSS)
- North American Electric Reliability Corporation (NERC)
Passwords – Are You Current and Secure?

Table 1

<table>
<thead>
<tr>
<th>Standard</th>
<th>Length</th>
<th>Cycle Time</th>
<th>Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>USGCB</td>
<td>12 Characters</td>
<td>60 Days</td>
<td>Alpha (Upper &amp; Lower) &amp; Numeric</td>
</tr>
<tr>
<td>FDCC</td>
<td>12 Characters</td>
<td>60 Days</td>
<td>Alpha (Upper &amp; Lower) &amp; Numeric</td>
</tr>
<tr>
<td>PCI-DSS</td>
<td>7 Characters</td>
<td>90 Days</td>
<td>Alpha &amp; Numeric</td>
</tr>
<tr>
<td>NERC</td>
<td>6 Characters</td>
<td>At least annually</td>
<td>Alpha &amp; Numeric &amp; Special</td>
</tr>
</tbody>
</table>

- Source: http://www.arellia.com/2013/04/30/password-strength-standards/

As can be seen, the criteria varies widely between standards, and you’ll note that none of the above include “8 characters”, which is part of what is arguably the most commonly accepted password practice:

Minimum of 8 characters with at least three of the following requirements:

- 1 upper case letter
- 1 lower case letter
- 1 number
- 1 special character
- Cycle time of 90 days.

There are additional, common guidelines for increasing the security of passwords:

- Increase the minimum length to 12 or 14 characters if possible
- Generate passwords randomly if possible
- Avoid repetitive patterns, dictionary words, letter and/or number sequences, usernames, family names, pet names, biographical information
- Include numbers and symbols if allowed
- Use capital and lower-case letters
- Avoid using the same password for multiple sites

---

8 Source: https://en.wikipedia.org/wiki/Password_strength
The greater the number of characters, the longer it would take to be cracked by algorithms, however not all applications support a large number of characters. Complexity requirements have conventionally been regarded as the most important factor for password security, however studies conducted in 2011 and 2012 have cast doubt on this. The studies demonstrated that user frustration increased significantly with complexity but less when it came to length; and that cracking algorithms “can be more easily thwarted by a long password that is created without number, symbol, or case requirements ...”

**Password Management**

One popular web comic brought an amusing perspective to password complexity:

![Password Management Comic](http://xkcd.com/936/)

This comic touches upon an aspect of passwords that users are all too preoccupied with: *memory*. As noted in the study referenced at the beginning of this paper, our problems with our memory isn’t with the complexity of a password/phrase it is with how many of them we have to remember. This has brought into popularity the password manager tools for our electronic devices such as tablets, computers, smartphones, and flash drives. Password manager tools are secure applications that allow you to record your passwords in one place, and you only have to remember one password to open it up and gain access. Password manager tools allow us to put less focus on memory and more on the retrieval process.

Password manager tools are a common and widely acceptable means of simplifying the use of passwords:

- No need to remember all of your passwords (the manager stores them securely)

---

Passwords – Are You Current and Secure?

- No need for manual re-entering of passwords (most managers can automatically enter passwords and keep them safe from key logger capture)
- Passwords are stored in an encrypted database
- Passwords can often be accessed on multiple platforms (tablet, PC, smartphone)
- Passwords can be auto-generated based on preset complexity criteria

There are many companies that have adopted an Enterprise password management system for maintenance and control of corporate passwords.

**Complexity and Cracking**

The comic also shows password entropy, a concept of information theory which gauges password strength in regard to resistance to brute force attack. Phrase-based passwords have higher entropy, and are considered to be more secure than a single password due to the greater number of characters used. However a challenge for implementing passphrases among enterprise users is that many software applications still do not support overly long or complex passphrases. Additionally, many password policies are still touting the requirement for mixed cases, numbers, and special characters and do not actively encourage the use of passphrases.

There are a multitude of password cracking methods in use today. Some you may have heard of such as include brute force attacks, dictionary attacks, and rainbow tables. Brute force applications will systematically analyze combinations of characters until a password is cracked. They require time. Dictionary attacks create passwords and their hashes which are indexed and referenced for future use. They require storage. Generating a password with a complexity of case, numbers, and symbols will strengthen passwords against most dictionary attacks (although dictionaries can grow based on experience with the various complexity combinations). Rainbow tables make use of algorithms and processing speed to more efficiently fast-crack passwords. They are a method used to “balance the time demands of brute force attacks and the storage demands of dictionary attacks.”

Additional methods of cracking involve phishing, social engineering, malware, offline cracking, shoulder surfing, spidering, and old fashioned guesswork. Tools and applications for cracking are extremely easy to acquire. This past March, the Ars Technica deputy editor, Nate Anderson (a cracking newbie) downloaded a list of over 16,000 hashed passcodes. Using only free software cracking tools and the internet, he managed to decipher nearly half of them in under a few hours. Turning this into a challenge Ars Technica turned the same list over to three more experienced hackers to see what they could do with it. Of the three (made up of a

---

10 Source: [http://identitysafe.norton.com/blog/blog/2013/06/10/top-5-reasons-you-need-a-password-manager/](http://identitysafe.norton.com/blog/blog/2013/06/10/top-5-reasons-you-need-a-password-manager/)


cracking software developer, a security consultant, and an anonymous cracker) all were able to attack the same list as Anderson with greater efficiency, and the top performer was able to crack 90% of the passcodes in just 20 hours.14

**Factors to Consider When Evaluating Password Policy**

We recommend that companies should consider several factors when evaluating a password policy:

- What is it you are securing with the password
- What is the risk and likelihood of an attack (including both external and internal sources)
- Are there regulations or other requirements that must be considered/met
- Does your system allow for long passwords or passphrases
- How much authority do you have over your user base

Secure Mentem surveyed the security staff of Fortune 500 companies to pinpoint some of the most successful aspects of raising security awareness. The result was a list of seven "notable habits:"15

1) C-Level support – Security awareness was a necessity for compliance and provided ROI.
2) Partnering with key departments – Legal, HR, Marketing, and Compliance departments can all provide additional resources and can help to drive security awareness.
3) Creativity – Particularly helpful for companies with a smaller budget.
4) Metrics – Create a baseline with studies of security-related incidents, surveys, and measurables.
5) Department of how – Demonstrate how employees can take more secure measures, rather than tell them what they should not be doing.
6) 90-day plans – Create a program to re-evaluate the security program and its goals every 90 days rather than annually.
7) Multimodal awareness materials – Incorporate a variety of tools into training with a focus on hands-on efforts employees can participate in.

In summary, password security standards and best practices continue to emphasize complexity as a preventive measure against cracking; however longer less complex passwords can be just as effective. Passphrases are generally regarded as the more secure method of authentication in comparison to passwords but are at the mercy of applications which may not currently support a large number of characters. Password Manager applications provide value where users are required to maintain a large number of passwords.

Education is always important.

---


About Kevin P. Martin & Associates

Kevin P. Martin & Associates is a CPA and consulting firm, offering a full spectrum of tax, audit, business and IT consulting, and risk and compliance services. We help organizations understand the increasing challenges they face, implement plans and controls that enable them to manage their risk and comply with the myriad regulations, and set them on a path for success and growth.

Whether it’s uncertainty in the marketplace, control failures, natural disasters or deliberate attacks from an adversary, KPM offers a variety of services to help you reduce your exposure. Our expertise extends to a variety of key risk and compliance issues including Business Continuity Planning, Disaster Recovery, Internal Audit, Sarbanes Oxley Preparation, Payment Card Industry (PCI), HIPAA, Life Sciences Regulatory Management, Data Center Review, Security Testing, Fraud Prevention, and FISMA.

Works Cited


