Abstract

Purpose – Using authentication to secure data and accounts has grown to be a natural part of computing. Even if several authentication methods are in existence, using passwords remains the most common type of authentication. As long and complex passwords are encouraged by research studies and practitioners alike, computer users design passwords using strategies that enable them to remember their passwords. This paper aims to present a taxonomy of those password creation strategies in the form of a model describing various strategies used to create passwords.

Design/methodology/approach – The study was conducted in a three-step process beginning with a short survey among forensic experts within the Swedish police. The model was then developed by a series of iterative semi-structured interviews with forensic experts. In the third and final step, the model was validated on 5,000 passwords gathered from 50 different password databases that have leaked to the internet.

Findings – The result of this study is a taxonomy of password creation strategies presented as a model that describes the strategies as properties that a password can hold. Any given password can be classified as holding one or more of the properties outlined in the model.

Originality/value – On an abstract level, this study provides insight into password creation strategies. As such, the model can be used as a tool for research and education. It can also be used by practitioners in, for instance, penetration testing to map the most used password creation strategies in a domain or by forensic experts when designing dictionary attacks.

Keywords Computer security, Strategies, Passwords, Classification, Categorization

Paper type Research paper

1. Introduction

In today’s world, information and communications technology (ICT) is tightly integrated with most individual’s lives. For our everyday life, using ICT to keep up with friends and family, keep track of personal economy, shopping, work and more is natural. Almost everyone is using their computers for work and in their spare time. One could argue that the online world has come to be a digital mirror of reality. Everything, in reality, has a place online. Much like having a lock and key to protect what is of importance in reality and passports to prove your identity, the ability of identifying yourself and what you are allowed to access is of high importance in the digital world. To prove one’s identity online, and thus, proving yourself to be the owner of the account, authentication is used (Nielsen et al., 2014). One of the easiest and, perhaps, most common ways to authenticate to a computer system is to use passwords (Nielsen et al., 2014; Houshmand and Aggarwal, 2017). In the digital world, a user commonly has a multitude of different passwords and when users create their passwords, they often use a strategy to make the password easy to remember (Zviran and Haga, 1990; Ur et al., 2015; Stobert and Biddle, 2014). As discussed by Pfleeger et al. (2015) this could be explained by the users being afraid that they will forget their passwords if they are too complex.
Passwords are also commonly used in data encryption. In this domain, a password can be seen as the means of encrypting and decrypting data and it is a practice that is becoming more and more popular among individual users. While encryption unarguably enhances the personal security it also poses a problem in the domain of digital forensics (Casey, 2011). As encryption makes data unreadable without the correct password, it makes it harder for practitioners of digital forensics to uncover data that can be used as evidence in criminal investigations (Kävrestad, 2017; Garfinkel, 2010; Vincze, 2016). As general awareness of security has risen, encryption is and will continue to be an issue within the domain of digital forensics (Al Fahdi et al., 2013; Shen et al., 2016). In forensic examinations, perhaps the most common way to tackle encrypted data is to use dictionary attacks to guess the correct password.

The purpose of this study is to develop a model that outlines a taxonomy of password creation strategies that provides a granular means of classifying passwords based on the strategy used to create them. In this study, password creation strategy refers to active approaches that can be used by a password creator to create memorable passwords (Zviran and Haga, 1990; Ur et al., 2015). The results of this study is a taxonomy that can be used to deepen the understanding of password types and password behavior. In the context of computer forensics, the model can assist in creating dictionary’s by visualizing the different existing strategies for password creation.

Increasing security awareness is an ongoing challenge for any organization (Furnell and Clarke, 2005). Using the taxonomy presented in this study, security practitioners can survey the password culture in an organization without disclosing the integrity of the actual passwords. This can, for instance, be done by a survey where the users are asked to self-classify their passwords, which can result in an overview of what passwords creation strategies that are used in the organization. Those results can then be used to tailor information and training according to the needs of the organization.

The study was executed in three steps. First, a survey and literature study was conducted to a draft a model of password creation strategies. Second, iterative semi-structured interviews with practitioners of digital forensics were used to develop the model. Finally, the model was further developed and validated by being applied to 5,000 actual passwords found in databases that leaked to the internet.

The rest of this paper is structured as follows. Section 2 discusses the motivation behind this study further. Section 3 describes the methodology used in this study. Section 4 presents the outcome of the study and Sections 5 and 6 presents a discussion on the results and possible directions for future work.

2. Motivation
As previously mentioned, using passwords is a very common type of authentication. Even with the advances in multi-factor authentication, strong passwords remains of outmost importance to repel attackers. As of today, almost any organization will be supported by IT, and the information security of that organization is, to some degree, dependent on secure authentication mechanisms being used by the users. As such, using various methods to influence or enforce the users to create strong passwords is a common practice that includes establishing written policies, using password meters and more (Wheeler, 2016). Another way to maintain the security of a computer system is by actually attempting to hack it to find weaknesses, an approach commonly known as penetration testing. As demonstrated by Morris and Thompson (1979), this practice has been in use for a long time. In a more recent example, Denis et al. (2016) argue that penetration testing is used to highlight security issues
and discusses that one common part of penetration testing concerns attempting to crack passwords.

A common practice in password cracking is the use of dictionary attacks. A dictionary attack involves using a list of possible passwords and using that list against the target account. As described by Narayanan and Shmatikov (2005) and Kyaw et al. (2015), a good dictionary attack involves anticipating the users’ password creation strategy and to mimic that in the creation of a dictionary. The taxonomy presented in this paper can be used as a reference material for creating dictionaries to use in penetration testing of user passwords, and as such help increasing the general password strength. Using dictionary attacks to crack passwords is also a common practice within the domain of computer forensics where the increased popularity of encryption software makes it harder to perform computer forensic examinations to investigate crimes (Freiling et al., 2018; Karie and Venter, 2015). As described by Tatli (2015), using efficient models for generating dictionaries is of importance when cracking passwords in the forensic domain. As such, the results of this study can also practically contribute to the forensic domain.

A core aspect of assuring a high level of security in any organization is to work toward a proper security culture. As discussed by Reid et al. (2014), that involves a proper password security culture and a part of achieving that is to provide the users with the training needed to manage password in a correct way. As described by Komanduri (2016), one way to improve the password culture is to construct password policies dictating how a password should be constructed. Our study outlines different password creation strategies and can be an aid in constructing such policies. Further, the results can be used as a tool to survey how the users in the organization actually construct their password, and therefore, be a part of password policy compliance work.

3. Methodology
This study was conducted in three steps beginning with a survey among forensic practitioners and analysis of background data gathered from the Internet and the research community. This step was not intended to provide all the information needed to create a complete model of all password creation strategies. Rather, this step provided information that was used to create a draft model used as input to the second step in the research process. In the second step, interviews were used to discuss the draft model with three computer forensic experts before the model was updated based on the information from the interviews. The interviews were held in a semi-structured fashion and then transcribed and analyzed using thematic coding, as described by Robson (2011). This second step was performed in an iterative manner and continued until all participants were satisfied with the model.

In the third step, the model was validated by manually applying it to 5,000 different passwords that were found by searching for databases of leaked passwords on the internet. In total, the validation included 50 databases with 100 passwords from each database. The passwords used were selected by taking the 100 first passwords in every database. However, if the database appeared ordered, every tenth password was selected to increase the randomness of the sample. Manual verification was selected in favor of automated verification as automated testing, if at all practical, would require quite sophisticated software development, outside the scope of this study.

Lincoln and Guba (1985) suggest the use of triangulation to produce reliable and dependable results. In this study, the concept of triangulation was built into the research design and implemented by including data from different sources and by holding the interviews separate rather than as group interviews. Including different data sources allows
for different views on the subjects to be included in the results and holding the interviews separately mitigate the risk of the participants being influenced by each other. Further, the study was designed to make the participants feel engaged to the study by continuously including the same participants in the iterative interview process. This conforms to the concept of prolonged engagement that should, according to Lincoln and Guba (1985), further increase the credibility of the results.

There have been several ethical considerations in relation to this study. The considerations that were most relevant was to consider how the conducted study could be abused and to make sure that the results cannot be harmful to people, as described by Schrittwieser et al. (2013). The research model that was used for this study included passwords from databases that were found online. Using this data does not pose a problem as the databases were already present online. However, to ensure that no information that could identify a user, a password or where the databases can be found, the description of the validation process is somewhat short and no found passwords are included in this paper. This does counter the high level of transparency that is feasible in a scientific publication. In this case, there is a trade-off between transparency and integrity of the password holders, and the integrity of the password holders must, in the author’s opinion, take precedence. One could also argue that the results themselves can be useful for harmful actions, such as influencing people that want to hide data to use even stronger passwords. However, as demonstrated in this paper, there are so many other sources of information that describes how to create strong passwords that the potential harmfulness of this study can be deemed as negligible.

Before moving on to the results of this study, it should be pointed out that the intent of this study is to survey password creation strategies. As demonstrated by, Wang et al. (2018) and Das et al. (2014), there are several other factors of importance in the domain of password security, including password reuse. However, this study is limited to the strategies used by users to create passwords and not how passwords are handled in general.

4. Results
This section presents the results of our study. First, the related literature used in conjunction with the survey to craft the draft model is briefly presented. Next, each step in the research process is presented in the upcoming sub-sections.

4.1 Related literature
Florencio and Herley (2007) present a study on password use and re-use habits. Using a client software shipped with a skew of Windows Live Toolbar, Florencio and Herley (2007) allowed users to opt-in to their study and gathered data from half a million users of over a three month period. They found that an average user has 6.5 passwords and each password is shared among 3.9 sites. Further, they also report that an average user has about 25 online accounts that require passwords and types 8 passwords per day. In this study, the password types lowercase, numbers, alphanumerical and strong passwords are mentioned. Strong passwords are being described as passwords of 6-13 characters in length containing upper and lowercase letters, numbers and special characters (Florencio and Herley, 2007).

SANS (2017) presents guidelines for constructing strong passwords. In the report “password construction guidelines” the need for using unique passwords for work accounts is stressed and SANS (2017) recommend the use of a password manager to keep track of multiple passwords. Further, a password length of at least 14 characters and the use of passphrases is recommended. The report mentions the following characteristics of weak passwords:
- passwords including biographical information (for instance, names, addresses favorite hobbies, etc.);
- passwords made up from patterns (typically patterns on the keyboard, for instance, qwertyuiop that is a straight line on a standard QWERTY keyboard); and
- passwords made up from combinations of words and number sequences.

Nielsen et al. (2014) highlight the benefits of password-based authentication as being the fact that it is easy to implement and easy to use for the end users. Further, this paper demonstrates that passphrases can be used to create longer passwords that are still easy for the user to remember. A variation of passphrases is mnemonic passwords. A mnemonic password is a password designed by constructing a phrase and letting one letter from each word in the phrase be used in the password (Kuo et al., 2006). To exemplify, a sample passphrase and the corresponding mnemonic password is presented below:

- **Passphrase** – Swedish midsummer includes eating potatoes and looking at polar bears roaming the streets.
- **Mnemonic password** – Smiepalapbrts.

Further, Kuo et al. (2006) attempted to crack a set of mnemonic passwords and found that mnemonic passwords were more resilient to dictionary attacks compared to non-mnemonic passwords.

Golla et al. (2016) present an attack that can be used to attack password managers that use honey encryption. Honey encryption is the practice of returning a plausible result in response to a password guessing attack that supplied an incorrect password. Of interest for this study is that Golla et al. (2016) mention the practice of using leetspeak as a way to modify characters in passwords to special characters to make the passwords more secure. Leetspeak was created as a community language, between hackers and others online, that only the people in the community could understand (Ross, 2006). Essentially, leetspeak is a written language where characters are switched for other characters or combinations of characters that visually resembles the original (Blashki and Nichol, 2005). Using leetspeak in password creation would involve creating a password and exchange characters in the password for other characters that are visually resembling the original characters. A common way to employ leetspeak is to substitute a lowercase “a” for an “@.” Table I presents a sample alphabet for leetspeak.

Zviran and Haga (1993) evaluated how well users could remember passwords that were created three months earlier. They found that even if only 27.2 per cent of the participants could remember passwords they created themselves, the recall rate of system generated passwords was even worse, only 12.7 per cent of the participants remembers system-generated passwords that was created three months earlier. However, they actually found

<table>
<thead>
<tr>
<th>Sample leetspeak alphabet</th>
<th>M = /V\</th>
<th>T = 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>A = @</td>
<td>G = 6</td>
<td>N = ^/</td>
</tr>
<tr>
<td>B = 8</td>
<td>H = #</td>
<td>O = 0</td>
</tr>
<tr>
<td>C = &lt;</td>
<td>I = 1</td>
<td>P = 9</td>
</tr>
<tr>
<td>D = (</td>
<td>J = .</td>
<td>Q = 0,</td>
</tr>
<tr>
<td>E = 3</td>
<td>K =</td>
<td>\</td>
</tr>
<tr>
<td>F = 1=</td>
<td>L = 1</td>
<td>S = 5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table I.</th>
<th>Sample leetspeak alphabet</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>M = /V\</td>
</tr>
<tr>
<td>A = @</td>
<td>G = 6</td>
</tr>
<tr>
<td>B = 8</td>
<td>H = #</td>
</tr>
<tr>
<td>C = &lt;</td>
<td>I = 1</td>
</tr>
<tr>
<td>D = (</td>
<td>J = .</td>
</tr>
<tr>
<td>E = 3</td>
<td>K = \</td>
</tr>
<tr>
<td>F = 1=</td>
<td>L = 1</td>
</tr>
</tbody>
</table>

A taxonomy of password creation strategies
that passwords that were pronounceable were easier to remember, with a recall rate of 38 per cent. While the statistics for different password categories is not the scope of this paper, it is notable that Zviran and Haga (1993) differentiate between passwords chosen by the user and system generated passwords. As further described by Fung et al. (1997), user-generated passwords are deemed weaker as users can choose short passwords or passwords existing in dictionaries. Sawyer (1990) describes that users often include private or personal information into the passwords making them even easier to guess. System-generated passwords, on the other hand, are often generated using a randomizer and are, as such, harder to guess but they are also written down more frequently (Zviran and Haga, 1990).

4.2 Creating a draft model
To create a draft model, the background material presented in the previous section was used together with a short survey sent out to forensic expert from the Swedish police. The intent of the survey was to gather information about what types of passwords that the forensic experts encountered in their everyday work. In total, 21 forensic experts responded to the survey and the information they provided was summarized to following password classes:

- phrases;
- biographical passwords;
- leetspeak;
- dates;
- words;
- combination of words and numbers; and
- random passwords.

In the literature presented in the previous section, it is notable that there are two high-level categories of passwords that have vastly different characteristics; user-generated passwords that are chosen by the user- and system-generated passwords that are created using the software. Further, several papers presented in the background literature describe that user-created passwords can contain information relating to the passwords holder, biographical information or be neutral to the password holder.

On a more detailed level, the background literature describes similar passwords characteristics as the survey and reflects that passwords can contain one or more of the following:

- small letters;
- only numbers;
- alphanumeric characters (numbers, small and large letters); and
- special characters.

It can be noted that the background literature and the survey, identifies that there are several approaches that can be used to create passphrases. These include using leetspeak that can be seen as using special characters and using mnemonic passwords that can appear to be random but are, in fact, derived from a phrase.

The intent of this step in the research process was to create a draft model, presented in Figure 1. The model is designed to contain different characteristics that passwords can hold and for the model to be successful, all passwords must contain one or more of the characteristics in the model. Based on the information gathered, it is clear that passwords
can be created either by humans or systems – this is also the first step created in the model. Passwords created by humans can either be neutral, meaning they are not tied to the password holder or biographic, meaning they include information relating to the password holder.

For each of the categories that describe who created the password, password characteristics were added. The characteristics that were added are intended to summarize the information presented throughout this section.

4.3 Interviews

The second step of the study consisted of interviews with forensic experts from the Swedish police. Three forensic experts were interviewed during this step and the interviews were held separately to avoid the participants influencing each other. Before each interview, the participant was handed the draft model and the interviews evolved around the strengths and weaknesses of the model. The interviews were transcribed and analyzed using thematic coding.

The analysis of the first round of interviews showed that “passphrases” and “alphanumeric characters” are categories that are very broad and that should be updated for increased granularity. This viewpoint aligns with the background information presented in Section 4.1. The interview participants suggested that a “passphrase” could be of any of the following different types: “leetspeak,” “word in word (a word inserted into another word, such as tom\textit{potato} ato)” and “mnemonic passwords”.

The participants also stated that plain words should have its own category with the same sub-categories as “passphrases” as neither “leetspeak” nor “mnemonic” or “word in word” is exclusive to actual phrases. As for “alphanumeric characters,” the participants thought that the following sub-categories should be added: “small letters,” “large letters,” “numbers” and “special characters” and that the “alphanumeric + special character” category should be removed.

The participants also discussed whether or not to include password length as a factor in the model. The general understanding was that while password length is definitely a factor in password complexity, it should not be included in the model. The subjects reasoning was

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure1.png}
\caption{A draft of the model of password classification}
\end{figure}

\textbf{Source:} Authors’ own
that password length is not a characteristic in the same way as the other characteristics reflected in the model.

After analyzing the interviews several modifications were made to the model, resulting in the model presented in Figure 2:

- Add “words” as a category.
- Remove “alphanumeric + special characters”.
- Add “special characters” under the category “alphanumeric characters”.
- Add “leetspeak” and “mnemonic passwords” under the category “words”.
- Add “word in word” under the categories “passphrases” and “words”.
- Add the category “patterns” to “neutral,” “user-generated” and “system-generated” passwords.

The model was sent to all participants for a second round. However, all participants stated that they were satisfied with the model.

4.4 Validation of the model
In the third and final step of the research process, the model was validated. In this step, 50 different databases containing passwords were found by using regular search engines on the internet. In total, 100 random passwords from each database were selected and classified using the model. No passwords were tested to see if they were actually real. Further, no passwords or database sources are published in this paper to maintain the integrity of the password holders. This is to comply with the ethical guidelines proposed by Schrittwieser et al. (2013). Table II presents the domains that the passwords appeared to be from.

During the validation, some passwords that could not be classified in the model in a satisfying way was encountered. At each of these occurrences, the model was updated so...
that the encountered passwords could fit into the model. When the validation process was completed the final model was sent to the interview participants from the previous step in the research process for feedback. None of the participants provided any information that suggested that the model should need further updates. The remainder of this section accounts for each change that was made to the model as a result of the validation. The final model is presented in Figure 6.

4.4.1 Adding special characters. One password that only contained special characters was encountered. As the model did not contain any category for special characters only, such a category was added as a sub-category to “biographic,” “neutral” and “system-generated” passwords. The change is shown in Figure 3 that shows the part of the model that concerns neutral passwords. Note that the parts of the model that concerns biographic and system-generated passwords are identical to the one reflecting neutral passwords.

4.4.2 Redesigning passphrases. Some of the passwords that were classified as passphrases could not be classified in a satisfying way. It became apparent that the category of passphrases has to be expanded to reflect the type of passphrase and the content of the passphrase. Some passphrases were in the form of mnemonic passwords or used leetspeak. Thus, these categories were added as sub-categories to “passphrases.” Further, it became evident that passphrases can contain words, numbers or special characters. These categories were added as sub-categories to “passphrases,” “leetspeak” and “mnemonic password.” The resulting model is demonstrated in Figure 4.

4.4.3 Redesigning words. Some of the passwords used in the validation process made it evident that “word in word” is a necessary sub-category to “words.” This change made it necessary to add “leetspeak” as a sub-category to “biographic,” “neutral” and “system-generated” passwords to be able to classify single words that used leetspeak. Finally, upper-

---

### Table II

<table>
<thead>
<tr>
<th>List of domains with leaked passwords used for validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>HBO</td>
</tr>
</tbody>
</table>

---

![Figure 3: The special characters category was added](image)

---

**Source:** Authors’ own
and lowercase letters were placed as sub-categories to the category “letters.” This approach will better reflect the possible content of passwords only containing letters. The “neutral passwords” part of the model is shown in Figure 5.

The resulting model reflects different characteristics that a password can have. All passwords should have at least one of the characteristics in the model and may hold more characteristics. For instance, one password may just contain special characters while a “word in word” password that was created using leetspeak will be classified as “word in word” and “leetspeak.” To exemplify the usage of the model, consider the passwords d00l1y1887 and SDF3234ºF#t5. The first one would be classified as biographical, leetspeak, letters and numbers because it contains elements of all those categories (assuming the owner is named dolly). The second would be classified as alphanumerical lowercase, uppercase, numbers and special characters.

5. Discussion
During the interviews held in this study it became evident that even if passwords remain the most common means of authentication, other means such as biometric locks and pattern locks are gaining in popularity. Also, combinations of authentication methods, multifactor authentication, is increasing in use. Considering other means of authentication was an ongoing discussion during this study, however, as the purpose was to study passwords.

**Figure 4.** Re-design of passphrases

**Source:** Authors’ own

**Figure 5.** Re-designed model of password classification

**Source:** Authors’ own
exclusively, other means of authentication has not been considered. While one could argue that surveying patterns, biometrics and more, passwords and password security will remain important and relevant in the future and studying all areas in-depth is, while important, not relevant in one study.

Another discussion was whether to include length as an aspect in classifying passwords. Related works, such as Florencio and Herley (2007) and SANS (2017), discuss password strength and number of characters, and password length is definitely an important factor in password security. Password length was, after analysis of the interviews, not considered in this study. The reasoning was that while the length is an important aspect of password security, length alone is not a new creation strategy that can be identified in any other way than to ask the password creator. Thus, the results gathered does not provide sufficient arguments to include length as a category.

Something that became clear during the validation process is that the success of the model is dependent on the person that uses the model. This means that depending on the user’s knowledge and background, different passwords may fall under different categories. This became very evident for cases where a password was classified by someone that did not understand the language that the password was written in. This could lead to passwords being categorized in the wrong category. For instance, consider a passphrase written in Finnish being analyzed by someone who does not understand Finnish. It is easy to see how this password can, by mistake, be categorized as a random alphanumeric string. However, this issue concerns the use of the model more than the model itself and it is unrealistic to expect the model to facilitate a solution for this type of issues. This also means that we cannot provide any meaningful statistics on the usage of different categories based on the analysis of existing passwords.

5.1 Societal contribution
As a tool that describes strategies for creating passwords, this study can have an impact on society in several ways. Most obvious is as a tool that can be used when discussing passwords in different settings, such as in education or when developing password policies in an organization. The results are also useful for computer forensic experts and penetration testers as a tool to use when creating dictionaries for dictionary attacks.

Using password policies and training is a common approach used by organizations trying to enhance the overall password security in their organization. A direct usefulness of this study would be to use the results to teach users about password creation strategies and promote the use of strategies that generates stronger passwords. Further, the taxonomy presented in this paper can be used to let the users self-categorize their passwords. The result of such a task could be twofold, first the user could get immediate feedback on their current passwords; and second, collecting the types of passwords used in the organization could provide an overview of the organizations’ current password security. As one example, a heat map of currently used strategies could be created and compared to a heat map of the organizations’ goals. This would create a graphical tool that can enable security managers to discuss password security with the users in an accessible manner.

5.2 Scientific contribution
The main scientific contribution of this study is the increased knowledge about password creation strategies and the model itself. As such, it is a tool that can be used by teachers and researchers to deepen the understanding of password creation strategies and passwords. It is notable that there has up until this time not been any established model on such a key point of security as passwords. Passwords are most likely the, by far, most used security
Figure 6.
The result of developing the model of password classification.
control in modern information systems and this model does help the scientific community to better understand passwords. Further, the model is a tool that can be used to further study the area of passwords and password security. As one example, the model can be used to study password habits by asking participants to classify their own passwords. That would allow for a study of user passwords without disclosing the actual passwords.

6. Conclusion

The aim of this study was to develop a model to classify passwords based on strategies used to create the password. The aim was met using a three-step research process that began with a survey that collected information about what types of passwords that had been encountered by computer forensic experts in Sweden. Data from the available literature were also collected in this step that resulted in a draft model that was used as input to the next step of the process.

In the second step of the research process, semi-structured interviews with forensic experts were used to further develop the model. The interview process was iterated until all participants were satisfied with the model. Including forensics experts that encounter passwords in their everyday work, and an interactive research design was used to make the participants feel engaged in the study and, as described by Lincoln and Guba (1985), generate more reliable results.

In the third step of the research process, the model that came out of the interview process was validated by applying 5,000 passwords from 50 different password databases to it. The validation process suggests that the model presented in this paper can, in practice, classify passwords based on password creation strategies, thus the aim of the study is met.

This study developed a model that describes different strategies for password creation. While several steps intended to ensure the completeness of the model was taken, one can never neglect the fact that other strategies than the ones included in the model may exist. That gives at hand that future work could include further development of the model using the same or other methods than the ones used in this study. Gathering additional data, in other contexts than in this study, could serve to strengthen and validate the model further. It is important to note that this model will need to be updated in the future as it is most likely that new and at this date, unknown password creation strategies will appear. Another possible direction is to expand the model into covering other types of authentication. The model can also be used as a tool in future studies. As such, the model can be used as a means to develop statistical studies to study, for instance, differences in password behaviors amongst persons from different cultures or genders or to investigate the most commonly used password creation strategies in a given population. Another way that the model could be used is to benchmark what password creation strategies that generate the most secure passwords. Adding such a study to the model would result in a model that can be used by organizations to visualize and decide how to create strong and memorable passwords.

The complete final model is presented in Figure 6.

References


Komanduri, S. (2016), “Modeling the adversary to evaluate password strength with limited samples”.


A taxonomy of password creation strategies

467

Sans (2017), “Password contraction guidelines”.

Corresponding author
Joakim Kävrestad can be contacted at: joakim.kavrestad@his.se

For instructions on how to order reprints of this article, please visit our website:
www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: permissions@emeraldinsight.com