Improving Usability of Password Management with Standardized Password Policies ♯

Bander AlFayyadh*, Per Thorsheim†, Audun Jøsang‡ and Henning Klevjer‡
*Queensland University of Technology, Australia
Email: b.alfayyadh@student.qut.edu.au
†EVRY, Norway
Email: per@thorsheim.net
‡University of Oslo, Norway §
Email: josang@mn.uio.no and hennikl@ifi.uio.no

***Abstract*—Recent studies indicate that many users have difficulties managing online passwords for the increasing number of accumulated accounts. As a result, users often adopt strategies to simplify password management, such as selecting weak passwords and reusing passwords across multiple accounts, which unfortunately can cause security vulnerabilities. This problem is exacerbated by the fact that users have to deal with many variations of password policy requirements even when dealing with similar service. This study investigates a set of password policies that a typical user would have to follow when selecting passwords for their various online services. We also investigate several authentication frameworks with regard to how they address password requirements as a function of authentication assurance levels. We find that password policies cause usability problems by not considering the authentication assurance level of the service, and by specifying diverging password requirements for service that have the same authentication assurance level. We conclude by presenting the skeleton of a possible unified standard passwords policy, and discuss issues related to achieving standardized password policies.**

I. Introduction

Users typically establish *ad hoc* strategies aimed at reducing the cognitive load of managing passwords for multiple accounts. With the increasing number of accounts that a typical Internet user accumulates it becomes increasingly difficult to keep separate passwords for each account, and to manage each password according to the respective password policies. In user studies on password habits [7], [12] it was found that while users accumulate more and more accounts as a function of the time they stay active online, the number of different passwords they maintain for accessing these accounts remains more or less constant. Password reuse is thus a very common practice which has the advantage of making it possible for people to manage and remember passwords for an increasing number of accounts. However, password reuse also represents a security vulnerability because it gives an attacker easy access to multiple accounts with a single stolen password.

In the study based on analyzing the real passwords of 544960 users by Florêncio and Herlay [6] it was found that during an 85 day period each user logged on to an average of 25 different accounts, and used an average of 6.5 different passwords, each of which was reused over 3.9 accounts. The average password entropy was 41 bits which approximately corresponds to 7 characters.

In the study based on interviews by Notoatmodjo and Thomborson on user perceptions about passwords [12], it was found that people tend to mentally classify accounts into different categories such as *high importance* accounts (e.g. online bank accounts), and *low importance* accounts (e.g. for reading online newspapers), and that password reuse is much more common for low importance accounts than it is for high importance accounts. Users thus have an intuitive understanding of the increased risk associated with password reuse, so they try to avoid it for sensitive applications such as online banking. The study concludes that educating users to never reuse passwords is unlikely to succeed. In order to maintain both adequate security and acceptable usability the study recommends that users instead should be encouraged to reuse passwords for low sensitivity applications, and be trained to recognize high sensitivity applications and to avoid reusing passwords for those.

According to the study on passwords habits by Adams and Sasse [3], it was found that insecure password practices can, in general, not be caused by user carelessness, but on the inadequacy of policies under which users have to manage passwords. There is an apparent dilemma between having lax and strict password policies. Lax policies are intuitively bad because they might allow short and insecure passwords. However, strict password policies can also be bad for security, for example, when passwords have to be changed frequently users tend to chose simple (not necessarily short) and thereby less secure passwords because it is the only way the cognitive load of remembering passwords can be made tolerable. For most people it would be too difficult to remember complex and theoretically secure passwords if they must be changed frequently. Requiring frequent password change for the purpose of strengthening password security has the paradoxical consequence of forcing users into the insecure practice of choosing simple passwords. The same study concludes that this can become a vicious circle whereby the IT security department introduces even stricter password policies which in turn forces users into even more insecure practices.

In a study on the effect of password policies on efficiency in user authentication by Inglesant and Sasse [10] it was found

that unreasonable and inconsistent requirements for password use creates unnecessary and costly overhead. For example it was found that the password security mechanisms cause stress from fear of forgetting passwords and the cumbersome password resetting procedures that would follow. It was further found that loss of time and insecure ad hoc practices are frequent results of inadequate password policies, and that the organizations surveyed in the study fail to realize that this overhead affects their productivity. Another cause of the mentioned requirements is that the total set of permutations the user can choose from is restricted, further reducing the entropy of the password. Using rules that force people to choose random (high-entropy) passwords from the whole password space thus has the paradoxical consequence that the available password space shrinks.

It is worth mentioning that SSO (Single Sign-On), RSO (Reduced Sign-On) and federated identity management are technologies that are currently being promoted to solve the growing problem of identity overload and password fatigue. In theory, SSO, RSO and identity federation makes it possible to use a single account and corresponding password to access separate accounts in a more or less transparent fashion. However, in practice these technologies are, and will only be used for accessing services within a domain of related service providers (SPs), or for bundling services [11]. SSO and RSO are typically implemented within the same organization or within the domain of closely related organizations. Identity federation requires legal agreements and a high level of trust between participating SPs. For political, commercial and security reasons it is unthinkable that all online SPs will federate into a single domain, or even a few domains. Despite the potential advantages of these technologies, there are no signs that the rate of accounts accumulation is slowing. In our opinion, SSO, RSO and Id federation will not solve the problem of identity overload and password fatigue, but represent methods for simplifying access to, and for bundling related services. We thus need to find other methods of solving this problem.

It is also worth mentioning local password management software that can be used to store usernames, passwords and other small pieces of sensitive information, such as account numbers. This type of software can be a simple function embedded in web browsers to store and automatically insert stored passwords into login pages, or it can be a separate dedicated software tool for storing and managing passwords and login information. This type of software can provide great usability benefits, but can also result in serious security vulnerabilities. Password policies typically prohibit passwords to be stored locally in Web browsers, (for example, expressed as: *"Always decline the use of the 'Remember Password' feature of applications*) [2]. While acknowledging that there are potential vulnerabilities with local password management we believe that specific types of this technology can lead to both increased usability and security.

In this study we analyze a set of contemporary password policies in order to determine whether they adequately take into account the reality of modern Internet users with a continuously increasing number of accounts with corresponding passwords. In this situation it is likely that an average user easily can accumulate hundreds of accounts during a lifetime of Internet activity. We feel that there is an urgent need to address this issue from a policy perspective. However, in a market driven environment this problem will not be addressed by single SPs because each SP only has the perspective of their domain, and so have little incentive to collaborate with potential competitors in order to draft more adequate password policies from a user perspective. This leads to the potential for standardization of password policies which in turn can be adapted by specific SPs and chosen by users. Such general policies must specifically take into account the fact that users continuously accumulate accounts and passwords, and must specify adequate practices for managing passwords in this environment.

II. Passwords in Authentication Frameworks

Differing sensitivity levels in different systems and applications leads to different risk levels associated with an instance of wrong authentication. The required authentication assurance level shall balance that risk, i.e. the higher the risk, the higher the required authentication assurance level. Authentication frameworks typically specify authentication assurance levels according to this principle. We have selected and analyzed the following four national/regional authentication frameworks regarding the use of passwords for authentication. Please note that theses frameworks are for the public sector and do not include military authentication.

- **US NIST SP800-63.** Title: *Electronic Authentication Guideline* [5]. This framework describes technical requirements for the authentication assurance levels that are specified in the E-Authentication Guidance for U.S. Federal Agencies [4].
- **EU IDABC.** Title: *eID Interoperability for PEGS (Pan-European eGovernment services): Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms* [8]. This is officially only a proposal, but is still widely adopted by subsequent EU policies and technical requirements, such as the STORK Quality authenticator scheme [9].
- **Norwegian FANR.** Title: *Framework for Authentication and Non-Repudiation in Electronic Communication with and within the Public Sector* [14]. This is the official authentication framework of the Norwegian Government. It is clearly inspired by the NIST framework above, but contains far less details.
- **Australian NeAF.** Title: *National e-Authentication Framework* [13]. This framework is the most recent and most advanced in this set of surveyed frameworks. NeAF adopts the authentication assurance levels of Queensland Government Authentication Framework (QGAF) [15] which explicitly includes AAL-0 which allows anonymous access as well as pseudonymous authentication.

Authentication Framework	*Authentication Assurance Levels*				
NIST (USA) 2006	Little or no assurance (1)		Some (2)	High (3)	Very High (4)
IDABC (EU) 2007	×	Minimal (1)	Low (2)	Substantial (3)	High (4)
FANR (Norway) 2008	Little or no assurance (1)		Low (2)	Moderate (3)	High (4)
NeAF (Australia) 2009	None (0)	Minimal (1)	Low (2)	Moderate (3)	High (4)

Fig. 1. Correspondence between authentication assurance levels in authentication frameworks

Fig.1 roughly compares the assurance levels of the mentioned authentication frameworks. It can be seen that there is a general consensus regarding the levels, although the NIST framework uses the terms ”High” and ”Very High” differently from the others, meaning e.g. that the assurance level NIST-”Very High” is equal to NeAF-”High”. This might be a source of confusion, so that practitioners who need to map the authentication assurance levels of systems between e.g. USA and Australia should be aware of the meaning behind the terms used in the respective frameworks.

It is interesting to see how the usage of passwords is specified in the various authentication frameworks. The tables below summarize the password requirements for each of AAL (Authentication Assurance Level) mentioned in Fig.1. Table I summarized password requirements for AAL-1.

Authentication Framework	**Password policy for AAL-1**
NIST (USA)	The probability of success of a targeted on-line password guessing attack by an attacker who has no prior knowledge of the password, but knows the user name of the target, shall not exceed 2^{-10} (1 in 1024), over the life of the password. There are no min-entropy requirements for Level 1. Passwords must never be transmitted in clear.
IDABC (EU)	Password or PIN token can be chosen by the claimant.
FANR (NO)	Password can be self-chosen password, and can be transmitted in clear over network.
NeAF (AU)	Can be based on memorized password, or or a list of passwords (code book), where both types must have a minimum entropy.

TABLE I
PASSWORD POLICIES FOR AUTHENTICATION ASSURANCE LEVEL 1

AAL-1 is typically used for services where the users self-register, meaning that it is not important to verify that the true identity of the user corresponds to the registered online identity.

Table II summarized password requirements for AAL-2.

AAL-2 is typically used when the application owner wants to verify that the trust identity corresponds to the registered identity, but that the consequences associated with false identity are still relatively low, which reduces the level of authentication assurance required.

Table III summarized password requirements for AAL-3.

Authentication Framework	**Password policy for AAL-2**
NIST (USA)	The probability of success of an on-line password guessing attack by an attacker who has no a priori knowledge of the password, but knows the user name of the target, shall not exceed 2^{-14} (1 in 16,384), over the life of the password. Level 2 passwords shall have at least 10 bits of min-entropy. Passwords shall never be transmitted in clear.
IDABC (EU)	Randomly generated password, PIN token or password list (but not passwords or PIN tokens chosen by the claimant).
FANR (NO)	Generated static or dynamic passwords (e.g. from precomputed list or from an unprotected OTP calculator).
NeAF (AU)	Memorized password, or list of passwords (code book), both with minimum entropy. Blocked account after a specific number of successive invalid passwords.

TABLE II
PASSWORD POLICIES FOR AUTHENTICATION ASSURANCE LEVEL 2

Authentication Framework	**Password policy for AAL-3**
NIST (USA)	Requires 2-factor authentication, where an OTP device can represent the 1st factor. The OTP output by the device shall have at least 10^6 possible values. The 2nd factor can be one of: • Authentication mechanism used to authenticate the claimant to the token, e.g. PIN or biometric. • The claimant sends the verifier (the hash of) a personal static password meeting the requirements for (E-authentication) Level 1 together with the one-time password. The personal static password must not be sent in clear. In addition, the verifier must be authenticated cryptographically to the claimant, for example using a TLS server. This is to avoid Man-in-the-Middle attacks.
IDABC (EU)	Requires 2-factor authentication, where 1st factor can be software or hardware based OTP generator. Static password not acceptable as 2nd factor.
FANR (NO)	Requires 2-factor authentication, where a static password and a list of static passwords (both generated by verifier) can represent one or both factors.
NeAF (AU)	Requires 2-factor authentication, e.g. list of generated passwords (code book) with minimum entropy, combined with authentication code diversification through shared secret.

TABLE III
PASSWORD POLICIES FOR AUTHENTICATION ASSURANCE LEVEL 3

AAL-3 is typically used when the consequence of false identity is significant, thereby requiring a relatively high level of authentication assurance.

Table IV summarized password requirements for AAL-4.

AAL-4 is typically used for applications where the consequences of false identity could be very high, thereby requiring the highest level of authentication assurance.

While there are similarities between the frameworks regarding the use of passwords, there are certainly many differences. For Level 1 for example, only NeAF mentions minimum entropy as a requirement (without specifying the exact entropy), and only NIST requires that the password shall not be

Authentication Framework	Password policy for AAL-4
NIST (USA)	Requires 2-factor authentication. Personal static passwords are not acceptable as a factor.
IDABC (EU)	Requires 2-factor authentication. Personal static passwords are not acceptable as a factor.
FANR (NO)	Requires 2-factor authentication, where the 1st factor must be asymmetric cryptographic hardware. The 2nd factor can be a generated static password or dynamic password (from protected OTP device).
NeAF (AU)	Requires 2-factor authentication. Personal static passwords are not acceptable as a factor.

TABLE IV
PASSWORD POLICIES FOR AUTHENTICATION ASSURANCE LEVEL 4

transmitted in clear.

For level 2, only NeAF requires that access be blocked after a specific number of unsuccessful attempts. NIST says that maximum 1 in 16,384 online guessing attacks should succeed against any online service. QAs protection against bruteforcing this would be inadequate, but can be adequate in an online environment when combined with e.g. limited number of failed authentication attempts.

For level 3, all frameworks require 2-factor authentication, where the 1st factor must be based on cryptographic hardware or software, and all frameworks except IDABC allow the 2nd factor to be a password.

For level 4, all frameworks require 2-factor authentication, where the 1st factor must be based on cryptographic hardware. Only FANR (Norway) allows the 2nd factor to be a password. This does not exclude that a personal static password can be used as a 3rd factor.

It can be noted that none of the authentication frameworks mention password reuse. However, this is specifically mentioned in the accompanying NIST framework *Guide to Enterprise Password Management* [16] which states:

> *There is generally no easy way to detect password reuse across systems, particularly when both internal and external systems are involved. To attempt to reduce the likelihood of password reuse, organizations can have their password management policies prohibit use of the same or closely-related passwords on organizational IT system and external systems. The password management policy can also explicitly forbid the reuse of centralized (e.g., domain) administrative level credentials with user or local (e.g., local administrator or root) accounts. Proper user training that stresses the importance of proper password management and protection and explains the risks of password reuse should also be implemented. However, without an enforcement mechanism, it is unlikely that policies against reuse will be significantly effective in reducing reuse, given the number of passwords that users typically need to remember.*

According to [16] password reuse can thus not be prevented, only discouraged. It is interesting to compare this with the advice given in [12] which says that password reuse should be encouraged for low sensitivity applications. It should be noted that the authentication frameworks listed in Fig.1 are aimed at authentication in relation to the public sector, and that these frameworks do not focus on purely personal or commercial applications. However, in our opinion, password reuse could be considered reasonable at AAL-1.

III. SURVEY OF PASSWORD POLICY CHARACTERISTICS

A. Brief Overview of Password Policies

The set of surveyed password policies represent typical password policies that a user would encounter in private and professional activities.

1) Wikipedia Password Policy: Wikipedia is the largest knowledge database on earth, and is created by the collaborative effort of around 100,000 regularly active contributors. Articles can be edited anonymously, where only the IP address is recorded, or can be edited by registered members of Wikipedia, where anybody can register with a self-chosen username and password. There is no explicit password policy, but the registration process enforces that the password must be at least 1 character long. We judge the authentication assurance level for Wikipedia to be AAL-1. The website can be accessed at: `http://en.wikipedia.org/`.

2) The New York Times Password Policy: The New York Times is a major online as well as paper-based newspaper, not just for New York but nationally in the US as well as internationally. Anonymous users can only read a limited number of articles per month (based on IP address). By registering, users can read an unlimited number of articles, and can subscribe to customized feeds. NY Times password policy is specified when signing up, but the registration enforces that the password length is 5-15 characters long. We judge the authentication assurance level for accessing the NY Times to be AAL-1. The website can be accessed at `http://www.nytimes.com`.

3) QUT Password Policy: Queensland University of Technology (QUT) is a major university in Australia with thousands of students and staff user accounts. We judge the authentication assurance level for accessing QUT services to be AAL-2. The surveyed QUT password policy was published on 18 October 2011 as a separate document, 2 pages long, that is available online from `http://www.its.qut.edu.au/governance/documents/PasswordPolicy252011.docx`.

4) UiO Password Policy: The University of Oslo (UiO) is Norway's largest university with thousands of students and staff user accounts. UiO is also member of the Norwegian national university identity federation network FEIDE, which technically can allow students and staff from other academic institutions in Norway to access services and resources at UiO. The password policies of those other institutions is outside the control of UiO. We judge the authentication assurance level for accessing UiO services to be AAL-2. The surveyed UiO password was published on 15 June 2010 as an online html document, approximately 1 page long, that is available from:

http://www.uio.no/tjenester/it /brukernavn-passord/passord.html.

5) eBay Password Policy: eBay is an online auction and shopping website in which people and businesses buy and sell a broad variety of goods and services worldwide. Founded in 1995, eBay is a multi-billion dollar business with operations localized in over thirty countries. According to eBay, they have 97 million active user and 5000 employees [1]. We judge the authentication assurance level using eBay services to be AAL-2. When creating an account, the user have the option to look at the password policy which can be found at: http://pages.ebay.com.au/help/new /contextual/create_password.html.

6) CitiBank Password Policy: CitiBank is a very large financial corporation located in the United States but with hundreds of branches all over the world. CitiBank customers can access their bank accounts using Its online service. We judge the authentication assurance level for online banking at CitiBank to be AAL-3. Their password policy can be found at: https://online.citibank.com /US/JRS/pands/detail.do?ID=SecurityUpdates.

7) Nordea Bank Password Policy: Nordea Bank is a major commercial and private bank in Norway. We judge the authentication assurance level for online banking at Nordea to be AAL-3. The bank also requires 2-factor authentication, where the first factor is a protected OTP device and the second factor is a static password. The password guidelines that we analyze here can be found at http://www.nordea.no/Privat /Internett+og+telefon /Råd+om+Internett+og+telefon /Sikkerhet+i+Nordea/783562.html.

8) Samba Financial Group Password Policy: Samba Financial Group is a major bank in Saudi Arabia. We judge the authentication assurance level for online banking at Samba to be AAL-3. The bank also requires 2-factor authentication, where the first factor is a protected OTP device and the second factor is a static password. The password guidelines that we analyze here can be found at http://www.samba.com/english/Common/HTML /PersonalInternetBanking_06_01_en.html

9) SANS Institute Password Policy Template: The SANS Institute is a security research and education organization. Its located in the United States but it holds various security training programs that reach more than 165,000 security professionals around the world. SANS is one of the largest sources for information security training and security certification in the world. It also makes available to the security community a free large collection of research documents about various aspects of information security. Their password policy is made available for anyone to use it and make changes if they wish. Because of its generality, the SANS password policy template does not reflect a specific authentication assurance level, but could typically be appropriate for AAL-2 or AAL-3. The policy is 3 pages in length and can be found at: http://www.sans.org/security-resources /policies/Password_Policy.pdf.

B. Summary of Password Policy Requirements

Table V summarizes the findings from the policies. The abbreviations used are explained in Table VI further below. All requirements are not included or specifically mentioned in each password policy. The case when a particular requirement is not mentioned is denoted as ”-” in Table V. Table VI explains the abbreviations used in Table V.

It is interesting to note the great variation in password requirements. None of the services explicitly indicate the sensitivity of the service. Instead, the users must themselves guess the sensitivity of the service. In Table V we have specified an estimated sensitivity level in the rightmost column. Studies show that users indeed estimate the sensitivity level of services [12], and that they tend to reuse passwords across low sensitivity services (AAL-1), but less so across high sensitivity services (AAL-3). We believe that it can cause confusion and security risks when users have to make this judgment themselves, and it would be advisable if SPs explicitly specify the sensitivity level of the service.

IV. Discussion

The investigation in Sec.II and Sec.III indicate that there are a wide range of different requirements for passwords. Defining one password policy for all situations would necessarily need to take into account the different requirements for different services. Similarly to the differentiation between password requirements according to AAL described in the authentication frameworks of Sec.II, a standard password policy could describe a set of password policies according to the authentication assurance level required.

Table VII summarizes a set of requirements and restrictions for passwords as a function of the AAL of the service that the password shall protect. As can be seen, the higher AAL, the more requirements and restrictions are specified. The abbreviations used are explained in Table VI.

Although most of the authentication frameworks of Fig.1 do not allow personal passwords for AAL-3&4 we have included it in Table VII because we believe it can be used as either a 2nd or a 3rd factor. Services at AAL-2 and AAL-3 would typically require a hardware device protected by a PIN or a biometric, which already represents two authentication factors. Nordea Bank uses a protected hardware device as well as a password, which then represents the 3rd factor. For AAL-3 and AAL-4 services the password strength should match the strength of the other factors.

There are many technical limitations of current password systems that limit the users’ ability to put entropy into their passwords. For example, many systems still do not allow special characters, do not differentiate between lower and and uppercase case characters, have a maximum password length of 8 characters, can not use any localized alphabet letters such as æ and ş, or can not start with a numerical character. These limitations in the composition of passwords are often caused by integrating password management across

Policy	Required length	Required character sets	Choice of character sets	Pwd. composition restrictions	Pwd. change frequency (months)	History restriction	Technical password mgmt	Password mgmt restrictions	Assumed AAL for service
Wikipedia	≥ 1	-	-	-	-	-	-	-	AAL-1
NY Times	$5-15$	-	-	-	-	-	-	-	AAL-1
QUT	≥ 8	= 4	L, U, N, S	BioX, DicX, SeqX	2	Y	stE, trE	-	AAL-2
UiO	≥ 8	≥ 3	L, U, N, S	BioX, DicX, UfiX, NlaX	11	Y	-	-	AAL-2
eBay Inc.	≥ 6	≥ 2	U, L, N, S	BioX, DicX, SeqX	-	-	-	-	AAL-2
CitiBank	≥ 6	≥ 2	C, N	BioX, DicX	2	-	-	-	AAL-3
Nordea Bank.	≥ 6	-	-	BioX, DicX	12	Y	-	AppX, ReuX, WriX	AAL-3
Samba Bank	≥ 8	= 3	C, N, S	BioX, DicX	-	Y	-	AppX, WriX	AAL-3
SANS	≥ 15	≥ 3	L, U, N, P, S	BioX, DicX, SeqX	3	Y	stE, trE	AppX	AAL-2,3

TABLE V
SUMMARY OF PASSWORD POLICIES

"-"	Means that requirement is not mentioned in the password policy
C	Alpha character with no distinction between Upper and Lower
L	Lower case character
U	Upper case character
N	Number character
S	Special character
P	Punctuation character (a type of special characters)
BioX	Biographic elements, e.g. name, user Id, date of birth, telephone
DicX	Dictionary word
SeqX	Sequence and repetition of characters, e.g. 123456, 333, abcdefg
stE	Stored password must be encrypted
trE	Transmitted password must be encrypted
Loc	Lock account after specific number of unsuccessful attempts
UfiX	Upper case character must not appear as first character
NlaX	Number character must not appear as last character
AppX	Applications (e.g. browser) must not be used to store passwords
ReuX	Reuse of password with other services is not allowed
WriX	Writing down passwords is not allowed
DerX	Deriving password from other password is not allowed
AAL	Authentication Assurance Level
Y	Yes

TABLE VI
ABBREVIATIONS USED IN TABLE V

heterogeneous systems, which results in the weakness of the "lowest common denominator", i.e. the resulting password policy can only contain requirements that are supported by all systems.

For online services, which very rarely enforce strong password policies (length, complexity, change frequency), it is very important to look at the problem from several perspectives:

- Services must store users passwords "securely" by using bcrypt, scrypt, pbkdf2 or similar. Many services still use MD5 which is broken and therefore insecure.
- Almost no matter the choice of hashing algorithms, passwords can be cracked online or offline unless minimum length password and/or complexity rules are enforced. Based on studies, around 40-50% of all users in any corporate environment will create passwords that have the very minimum length and complexity of the technically implemented password policy. In other words, corporate users will usually try to get away with the simplest passwords they can.
- Many sites also give a policy, or at least recommendations on screen, but do not really enforce them. As a result, any standard auditor will see the service policy as sufficient. Without further tests or "password cracking" to verify compliance, security will NOT be sufficient or compliant.
- More and more online services are based on newer products, software and systems, which in general tend to allow both complexity, national characters and lengths that exceed 10, 12 or 15 characters. This makes it easier to apply a general password policy as we suggest.
- An area that has received relatively little attention is the estimated cost of fixing systems that today do not allow for any decent password policy to be implemented. By decent we mean that the system should allow for up to 64 character length passwords, unicode character support and minimum lengths of at least 10 characters.
- Current computation power makes it relatively easy and cheap to generate rainbow tables for cracking passwords of length up to at least 8 characters of mixed character sets. Password length of 8 characters can therefore not be considered secure.
- The average time between password changes in most corporations is typically "too often". The result of that is that many users practice a +1 increment to their password. By using Levenshtein edit-distance metrics to analyze generations of passwords (up to 24 back in time), it is often found that the "+1" is part of the standard password procedure of many users.

A general observation that can be made from usability studies on personal passwords management is that passwords should be written down somewhere. The relatively large

Policy	Required length	Required character sets	Choice of character sets	Pwd. composition restrictions	Pwd. change frequency (months)	History restriction	Technical password mgmt	Password mgmt restrictions
AAL-1 Policy	≥ 5	-	-	-	-	-	-	-
AAL-2 Policy	≥ 8	≥ 2	L, U, N, S	BioX, DicX, SeqX	13	never	stE, trE	AppX
AAL-3 Policy	≥ 13	≥ 3	L, U, N, S	BioX, DicX, SeqX	26	never	stE, trE, Loc	AppX, ReuX
AAL-4 Policy	≥ 15	$= 4$	U, L, N, S	BioX, DicX, SeqX	39	never	stE, trE, Loc	AppX, ReuX, DerX

TABLE VII
PASSWORD POLICIES ACCORDING TO AUTHENTICATION ASSURANCE LEVEL

number of passwords that the average user maintains makes it impossible to memorize all passwords. The question is whether passwords should be written on digital or paper media, and how such media should be kept. Storage on a digital device can be in clear as long as the device is always offline. For online devices, the passwords must always be stored in encrypted form. Writing passwords in a paper notebook would require that the notebook be kept safe. As an additional precaution it is advisable to make the existence of passwords in a notebook appear non-obvious. For example, avoid indicating the presence of passwords by writing a title like ”Passwords”.

One paradoxical observation is that it might be counterproductive to recommend specific methods for password storage because it could give attackers knowledge about places to search for passwords if such specific recommendations were adopted by users in general.

We recommend that password reuse for AAL-1 services, and related password derivation schemes for AAL-2 services should be acceptable. However, for AAL-3 and AAL-4 services passwords should be truly unique for each service.

By officially making it acceptable to write passwords down it becomes less demanding to chose complex passwords, which also takes away the fear of forgetting passwords.

V. CONCLUSION

This paper analyses password policies from different institutions, companies and websites. Some of these policies are presented as a set of guidelines or advice, and not as mandatory rules. We have also compared the password requirements of prominent authentication assurance frameworks.

Password policies vary in many ways. There were similarities and differences in the requirements of the policies we examined. However, we have not found consistent password policy requirements. It is noticeable that large commercial websites such as yahoo or eBay have lax password policies that are only partially enforced. Some websites go as far as to enforce only the length rule while permitting passwords such as ”123456” even though it specifically states in its policy that this is a bad password. Examining the four national/regional authentication frameworks, we identified a harmonization of the authentication assurance levels. This leads us to suggest that harmonized password policy should be defined, which if endorsed by governments and institutions similar to the ones investigated may be adopted by government and private sector organisations. The password required password strength should be a function of the authentication assurance level of the service. Many technical restrictions stand in the way, for example compatibility with old systems that still do not differentiate between lower and upper case, or do not allow special characters. Another problem is that different languages have different character sets that may make it hard for certain characters to be available on all keyboards or computers. However, we believe in striving towards harmonized password policies – which might not fit for all applications – but which would provide an alternative to the many variations of password policies that exist today.

None of the studied password policies makes any reference to any of the authentication frameworks. In addition, the authentication frameworks provide little advice regarding password management. We believe that it would be advantageous to define a general password policy that expresses requirements for each specific authentication assurance level. Service providers can then specify the authentication assurance level of a given service, and simply refer to the corresponding requirements of the general password policy. This would simplify the problem of password management for users because they do not need to relate to different password policies for each service. Instead, they will immediately know how to handle a password when they are informed about the authentication assurance level of the service.

In future research we will investigate personal password management habits related to where people tend to store passwords, and which protection measures people employ. Instead of recommending specific methods for managing passwords we would like to be able to provide general advice on which methods that should be avoided and which methods that are acceptable. The goal is to identify personal password management methods that are both user friendly and secure.

REFERENCES

[1] eBay: Online Auction Website. url{http://www.ebayinc.com/assets/pdf/fact_sheet/GSI-CorpOverview_9.09.11.pdf}.

[2] SANS Password Policy. url{http://www.sans.org/security-resources/policies/Password_Policy.pdf}.

[3] Adams, Anne and Sasse, Martina Angela. Users are not the enemy. *Commun. ACM*, 42:40–46, December 1999.

[4] Joshua B. Bolten. E-Authentication Guidance for Federal Agencies – Memorandum to the Heads of All Departments and Agencies (M-04-04). Technical report, Executive Office of Tthe President, Office of Management and Budget, Washington, D.C. 20503, 2004.

[5] William E. Burr, Donna F. Dodson, and W. Timothy Polk. Electronic Authentication Guideline – NIST Special Publication 800-63. Technical report, National Institute of Standards and Technology, 2006.

[6] Dinei Florencio and Cormac Herley. A Large-Scale Study of Web Password Habits. In *Proceedings of the 16th International Conference on World Wide Web (WWW'07)*, pages 657–666, New York, 2007. ACM.

[7] Shirley Gaw and Edward 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, 2006. ACM.

[8] Hans Graux and Jarkko Majava. eID Interoperability for PEGS (Pan-European eGovernment services) – Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms. Technical report, EU IDABC (Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens.), 2007.

[9] B. Hulsebosch, G. Lenzini, and H. Eertink. Deliverable D2.3 - STORK Quality authenticator scheme. Technical report, STORK eID Consortium.), 2009.

[10] Philip Inglesant and Martina Angela Sasse. The true cost of unusable password policies: password use in the wild. In Elizabeth D. Mynatt et al., editors, *CHI 2010*, pages 383–392. ACM, 2010.

[11] A. Jøsang, M. AlZomai, and S. Suriadi. Usability and Privacy in Identity Management Architectures. In *The Proceedings of the Australasian Information Security Workshop (AISW), CRPIT Volume 68*, Ballarat, Australia, January 2007.

[12] Notoatmodjo, Gilbert and Thomborson, Clark. Passwords and perceptions. In *Proceedings of the Seventh Australasian Information Security Conference (AISC 2009*, pages 71–78. Australian Computer Society, Inc., 2009.

[13] Department of Finance and Deregulation. *National e-Authentication Framework (NeAF)*. Australian Government Information Management Office, January 2009.

[14] Ministry of Government Administration Reform. Framework for Authentication and Non-Repudiation in Electronic Communication with and within the Public Sector (in Norwegian: Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor). Technical report, Norwegian Government, 2008.

[15] Office of Government ICT. *Queensland Government Authentication Framework (QGAF)*. Queensland Government, October 2006.

[16] Karen Scarfone and Murugiah Souppaya. Guide to Enterprise Password Management (Draft) – NIST Special Publication 800-118. Technical report, National Institute of Standards and Technology, 2009.

(♯) Appears in the proceedings of SAR-SSI 2012: 7ème Conférence sur la Sécurité des Architectures Réseaux et Systèmes d'Information (7th Conference on Network and Information Systems Security), Cabourg, May 2012.

(§) The work reported in this paper has been partially funded by the Franco-Norwegian Foundation Project 1/11-FNS, and by the EUREKA Project 7161 Lucidman.