# Text Password Survey: Transition from First Generation to Second Generation

Gayathiri Charathsandran
University of British Columbia, Vancouver, Canada
cgaya@mss.icics.ubc.ca

## ABSTRACT
Text passwords are well-established, most widely used today, despite of many alternatives proposed to replace text passwords to date. Text password research has three decades of history and a recent research shows new paradigm in usable text passwords criticizing the past history. We provide a comprehensive overview of published research in text password schemes in two era, covering usability, security and deployability aspects, as well as system evaluation based on usability, deployability and security benefits that an ideal scheme might provide. The paper first catalogues existing web authentication scheme approaches, highlighting novel features of selected schemes and identifying key usability, deployability or security benefits. We then evaluate the usability, security and deployability requirements satisfied by the schemes in both eras, identify security threats that such systems must address, discuss usability issues and review known attacks. Finally we discuss the transition between the two eras and the future research direction and requirement of the text password schemes.

## Categories and Subject Descriptors
K.6.5 [**Management of Computing and Information Systems**]: Security and Protection—*Authentication*; H.1.2 **[Models and Principles]**: User/Machine Systems—*Human factors* H.5.2 [**Interfaces and Representations**]: User Interfaces— *User-centered design*

## General Terms
Security, Human Factors

## Keywords
Authentication, text passwords, usable security

## 1. INTRODUCTION
Text-password based authentication schemes are a popular means of authenticating since last 4 decades, for its easiness, cost effectiveness, simplicity and familiarity to all users 1010. Text passwords are text-based (memometrics) mechanism (see Figure 1). They contain alphanumeric and/or special keyboard characters and it was used as a shared secret by the user to authenticate her/himself to the system.

Over forty years of research have demonstrated that passwords are plagued by security problems 10 and openly hated by users10, regardless of many improved text password schemes proposed to date 10101010.

Many text password choice methods have been proposed to improve password memorability and thus usability, while at the same time improving strength of the password to prevent against guessing attacks 101010, nevertheless most users continues to choose poor quality passwords, re-use and forget them in great deal 10.

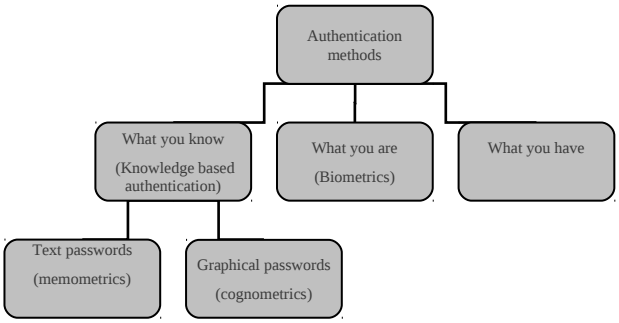


**Figure 1 Knowledge-based authentication 10Error: Reference source not found**

Many alternative schemes been proposed as an alternative to text password to improve usability and security. Two decades of stories on how urgent and imperative it is to replace them has had little impact: stronger alternatives and two-factor schemes are relegated to fringes 10. End user authentication technologies involving biometrics and tokens 10, client side public key infrastructure 10 and graphical variations of passwords 10 largely failed to mainstream deployment. Yet Another Authentication Scheme (YAAS), new schemes to replace passwords, are offered with regularity but expectations of success are so slow 10. Namely, OpenID has little evidence of user adaptations 10, Object based passwords 10 has immerged recently and little is known yet and many other schemes 10.

C. Herley and P.C. van Oorschot argue that no silver bullet will meet all requirements, and not only will passwords be with us for some time, but in many instances they are the solution which best fits the scenario of use 10. C.Herley, PC.van Oorschot, J. Bonneau, C. and F. Stajano, shows that selected scheme authors for their benefit analysis in their survey paper, are not only optimistic but also incomplete, using the framework they have defined. Also their evaluation of alternatives schemes compared to the text passwords shows that; most schemes do better than passwords on security, some schemes do better and some worse on usability and every scheme do worse than passwords on deployability 10.

Cormac Herley argues that most security advice simply offers a poor cost-benefit tradeoff to users and the users' rejection of the security advice they receive is entirely rational from an economic

perspective 10. So the password security community has looked back the research history of password security and usability and came up with new paradigms of solutions and yet shows that the text password practice won't end soon 10.

Contributing to the nascent literature on soft paternalistic solutions to security and privacy problems, experiment results shows that when given a valid explanation for a security delay, people will tolerate it 10 and the sites with the most restrictive password policies do not have greater security concerns; they are simply better insulated from the consequences of poor usability 10. Hence, new password schemes were proposed in support of recent literature 10.

We categories schemes based on password mechanism goals: *password strength, password diversity, password management, password theft, and password composition*. All the schemes we selected try to improve one of the goals of password security and in contrast password composition we mention at last discuss about the password policies. Password policies discuss the overall password strength as a whole. We discuss the categories of scheme in two generations. First generation password schemes were discuss in *Section 6* and second generation of passwords schemes were discussed in *Section 7*. We also discussed the overview of the text password usability, depolability and security in general in *Sections 2, Section 3* and *Section 4* respectively. We used the survey papers conducted on security and usability of text passwords to discuss *Section 2* and *Section 4*. However, deployability is a new parameter and was not discussed explicitly in past papers, even though the concept was in practice and some paper talked about it implicitly. We discuss about the parameters we choose to measure the benefit of schemes over one another in *Section 5*. *Sections 8 discuss* about the transitional changes between two generation of passwords and finally *Section 9* discuss the summary of the findings.

Our present work does consider the machine-to-machine authentication schemes and doesn't consider the challenge response schemes of user-to-machine text-password schemes. Our schemes selection is based on the improvement made on the schemes in each category.

## 1.1 Scope of this paper

The literature has documented many methods of implementing and improving security of text password mechanisms. Improvement can be viewed in two categories; *Protocol Improvement* and *Design Improvement*. Protocol improvement schemes are proposed to improve machine-to-machine password exchange security 10. Design improvement schemes are proposed to improve the user-to-machine secure password selection or password entry. We are interested in surveying un-cued recall based schemes. Passwords in un-cued recall can be classified into *user generated passwords* and *system generated passwords*. *User generated passwords* are passwords user type in the interface. *System generated passwords* are passwords, generated by automated systems and are called "password generators" (Eg: ALPHANUM, DICEWARE and PRONOUNCE3 10). We have narrowed down our scope to user generated text passwords schemes only (refer Figure 2).

Motivation of this survey is in multifold. First we analyze the text password schemes proposed in the first and second generation of passwords, based on the usability, security and deployability benefit parameters framed in the recent survey 10. We then identify security threats that such systems must address and review known attacks, discuss usability issues.

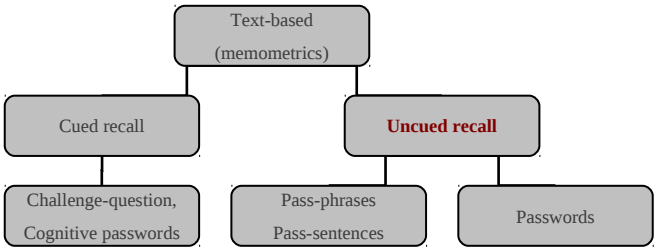


**Figure 2 Text-based password schemes 10**

Finally we identify and discuss the transition happened between first and second generations of passwords and discuss some open questions and research directions of text password.

We classified this paper into two eras. We have considered the password schemes proposed supporting the legacy theory of password security as *first generation text password schemes.* Schemes which were proposed based on C. Herley's advice 10 as *second generation text password schemes.*

# 2. SECURITY

Since Feldmeier and P. Karn, pointed that the single most important step that can be taken to improve password security is by increasing the entropy 10, there had been many proposals introduced to improve the security of the passwords. But the past history of text password proposals shows that, text passwords score relatively poorly on security, compared to other alternative schemes.

Text passwords can be used to impersonate a user after observing them authenticate using keyboard. Attackers can do shoulder surfing attacks and dictionary attacks by filming the keyboard 10, record the keystroke sounds 1010 or use the thermal image of the keyboard to obtain the password 10.

User-selected passwords are subject to statistical guessing attacks, a form of dictionary attack, in which an attacker sorts the password dictionary by presumed, or previously observed, popularity and guesses the most popular passwords first 10 10. Frequent for user-chosen secrets to be selected from a small and well-known subset (low min-entropy) throttled to guessing attack 10.

Attacker also can impersonate a user by intercepting the user's input from inside the user's device (e.g., by keylogging malware) 10 or eavesdropping on the clear text communication between prover and verifier while user is typing the password.

The fact that users reuse the text passwords across sites 10, leads to successful attack on insider fraud at one provider, or one back-end, endangers the user's accounts at other sites, as even a properly salted and strengthened hash function 10 can't protect many passwords from dedicated cracking software.

Text password schemes vulnerable to more sophisticated real time man-in-the-middle or relay attacks, in which the attackers have one connection to the victim prover (pretending to be the verifier) and simultaneously another connection to the victim verifier (pretending to be the prover) 10.

Mostly OpenID, password Managers, Microsoft passport, paper tokens, Visual crypto, Hardware token and Phone based passwords schemes are better than text password schemes.

## 3. USABILITY

Usability of text passwords was mostly concern as a major issue when alternative schemes like graphical and cognitive passwords began to immerge, but they fails to compete the text passwords 10.

The difficulty of guessing passwords was studied over three decades ago 10 with researchers able to guess over 75% of users' passwords; follow-up studies over the years have consistently compromised a substantial fraction of accounts with dictionary attacks. A survey 10 of corporate password users found them flustered by password requirements and coping by writing passwords down on post-it notes. On the web, users are typically overwhelmed by the number of passwords they have registered. One study 10 found most users have many accounts for which they've forgotten their passwords and even accounts they can't remember registering. Another 10 used a browser extension to observe thousands of users' password habits, finding on average 25 accounts and 6 unique passwords per user. Thus, passwords, as a purely memory-based scheme and must be remembered and chosen for each site 10.

Usability of biometrics passwords, password managers, OpenID and Microsoft passports are noticeably better than text passwords schemes 10.

## 4. DEPLOYABILITY

Text passwords are most used system today. No other schemes proposed to replace them failed, and thus not widely used commercially. The main reason is as they cost more, if the user wanted to use it. Even though text passwords are vulnerable guessing attack and brute force attack, text passwords remains the most prominently used scheme. This is because deployability itself doesn't determine the password strength, but also usability and security. There is a trade off between these parameters. To achieve creating a strong password we need to achieve considerably in all these parameters (see Figure 3**)**.

## 5. "UDS" BENEFITS

We use the benefits parameters defined to the text password by J. Bonneau, C. Herley, P.C. van Oorschot and F. Stajano 10, which is derived from the web password schemes discussed in web password survey 10. We have used some of those parameters and some parameters we learned from the schemes we surveyed to analyze the schemes. The benefits we consider are divided into three categories: usability, deployability and security.

When rating text-password schemes we assume that implementers use best practice such as salting and hashing, even though they often don't used in practice 10.

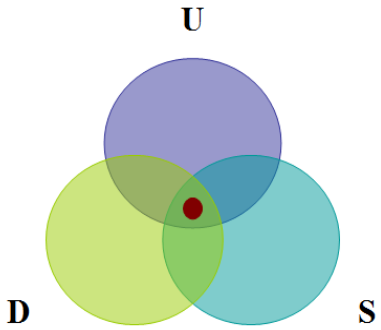


**Figure 3 UDS property**

### 5.1 Usability benefits

U1 *Nothing-to-Carry*: Users do not need to carry an additional physical object (electronic device, mechanical key, piece of paper) to use the scheme. Quasi-Nothing-to-Carry is awarded if the object is one that they'd carry everywhere all the time anyway, such as their mobile phone, but not if it's their computer (including tablets).

U2 *Easy-to-Learn*: Users who don't know the scheme can figure it out and learn it without too much trouble, and then easily recall how to use it.

U3 *Efficient-to-Use*: The time the user must spend for each authentication is acceptably short. The time required for setting up a new association with a verifier, although possibly longer than that for authentication, is also reasonable.

U4 *Infrequent-Errors:* The task that users must perform to log in usually succeeds when performed by a legitimate and honest user. In other words, the scheme isn't so hard to use or unreliable that genuine users are routinely rejected

U5 *Easy-Recovery-from-Loss:* A user can conveniently regain the ability to authenticate if the token is lost or the credentials forgotten. This combines usability aspects such as: low latency before restored ability; low user inconvenience in recovery (e.g., no requirement for physically standing in line); and assurance that recovery will be possible, for example via built-in backups or secondary recovery schemes. If recovery requires some form of reenrollment, this benefit rates its convenience.

### 5.2 Deployability benefits

D1 *Accessible:* Users who can use passwords3 are not prevented from using the scheme by disabilities or other physical (not cognitive) conditions.

D2 *Negligible-Cost-per-User:* The total cost per user of the scheme, adding up the costs at both the prover's end (any devices required) and the verifier's end (any share of the equipment and software required), is negligible. The scheme is plausible for startups with no per-user revenue.

D3 *Server-Compatible:* At the verifier's end, the scheme is compatible with text-based passwords. Providers don't have

to change their existing authentication setup to support the scheme.

D4 *Browser-Compatible:* Users don't have to change their client to support the scheme and can expect the scheme to work when using other machines with an up-to-date, standards-compliant web browser and no additional software. In 2012, this would mean an HTML5-compliant browser with JavaScript enabled. Schemes fail to provide this benefit if they require the installation of plugins or any kind of software whose installation requires administrative rights. Schemes offer Quasi- Browser-Compatible if they rely on non-standard but very common plugins, e.g., Flash.

D5 *Mature:* The scheme has been implemented and deployed on a large scale for actual authentication purposes beyond research. Indicators to consider for granting the full benefit may also include whether the scheme has undergone user testing, whether the standards community has published related documents, whether open-source projects implementing the scheme exist, whether anyone other than the implementers has adopted the scheme, the amount of literature on the scheme and so forth.

D6 *Non-Proprietary:* Anyone can implement or use the scheme for any purpose without having to pay royalties to anyone else. The relevant techniques are generally known, published openly and not protected by patents or trade secrets.

## 5.3 Security benefits

S1 *Resilient-to-Password Reuse:* It is not possible for a user to reuse the password in across the websites, as it will leads to attack on compromising the password. However if a scheme allow password reuse and have a mechanism to prevent the password being compromised or reduce the attack against password, then we say such mechanism is *Resilient-to-Password Reuse.*

S2 *Resilient-to-Guessing attack:* If the scheme is strong enough to prevent guessing attack then we say such scheme is *Resilient-to-Guessing attack*.

S3 *Resilient-to-Physical observation:* If the scheme is strong enough to prevent shoulder surfing attack, then we say such scheme is *Resilient-to- Physical observation*.

S4 *Requiring-to-Dictionary attack:* If the scheme can prevent dictionary surfing attack, then we say such scheme is *Resilient-to- Dictionary attack*.

S5 *Requiring-to-Brute force attack:* If the scheme can prevent the attacker performing brute attack against text password, then we say such scheme is *Resilient-to- Brute force attack*.

S6 *Requiring-to-Internal Observation:* If the scheme can prevent the attacker compromising the password using leylogger, then we say such scheme is *Resilient-to-Internal Observation.*

S7 *Requiring-to-Social Engineering attack:* If the scheme can prevent the attacker compromising the password using social engineering techniques, then we say such scheme is *Resilient-to- Social Engineering attack*.

*S8 Requiring-to-Phishing attack:* If the scheme can prevent the attacker compromising the password by phishing the website, then we say such scheme is *Resilient-to-Phishing attack*.

# 6. FIRST GENERATION SCHEMES

Robert Morris and Ken Thompson published the first academic paper on password security in 1979 10. They presented empirical analysis of users' password choices by conducting dictionary attacks on a real system. Since then password security research has been studied extensively and new improved schemes have been proposed alternatively. Sasse, Brostoff and Weirich 10 refer the users as the weakest link in the security chain. Allan, A. 10 argues that passwords are near the breaking point and suggested to consider using stronger authentication methods, rather than increasing the length and complexity of passwords. Wide-range of usability studies have been conducted on password usable security 10. Recently C.Herley 10 states that, users are not irrational and security researcher has to present a better tradeoff if we want a different outcome. His other papers related to his theory of security of passwords, reviewing the past history extensively argues and proves very interesting results to the research community. We discuss this in detail in Section 7.

Hence we considered the papers which followed the legacy theory of secure passwords, as first generation of passwords. However, some papers recently published as well falls into this category. So we don't want to precisely define the period of these generations, but looked at it as transition between these periods. This first generation category of papers, mostly considered security parameters as the main factor to improve the security of the passwords, even though it discuss about the usability of schemes proposed. Usability had been given more importance and studied expensively, in the later part of this era. This leads to the second generation of the passwords.

**Thus, first generation of passwords considered, password security rely on security and usability of the password and there is a tradeoff between them**.

The schemes we discuss here are categorized based on the goals of the password security mechanisms each category attempts to improve. First generation of text passwords proposals are immense and it is hard to discuss everything in a single paper. Hence we have chosen limited papers and narrow down our scope of the survey.

**Text password** it self is a single scheme. Password composition mechanism is very simple.

- User choose an easy to remember password
- Use the password to authenticate

However, password security researchers realized the weakness of the user's independent passwords, identified the vulnerability and suggested improved security measures. David L. Jobusch and Arthur E. Oldehoeft reviewed the goals of authentication, and the strengths 10 and vulnerabilities of text password mechanisms are discussed 10, in UNIX system.

## 6.1 Password strength

Weak passwords chosen by the users can be vulnerable to guessing attack. The schemes presented here are proposed to overcome the *guessing attack* and *brute force attack* and yet to guide selecting strengthen passwords. Shannon's 10 model of entropy for encoding language into bits is used to measure the strength of the passwords.

General mechanisms of these schemes:

- User select short passwords with high entropy

Random passwords are composed of random sequence of letters with high entropy and hard to crack. Sundararaman Jeyaraman and Mercan Topkara 10 suggested a mnemonic generator based on a text-corpus to generate mnemonic passwords. Umut Topkara Mikhail J. Atallah Mercan Topkara 10 suggest that, instead of using the mnemonics generator, mnemonic sentence can be generated to helps the users remember a multiplicity of truly random passwords and which are independently selected. Alain Forget, Sonia Chiasson, P.C. van Oorschot, Robert Biddle 10 proposed Persuasive Text password (PTP) scheme (Figure 4) which let the users to shuffle to be presented with randomly-chosen and positioned characters until they find a combination they feel is memorable.

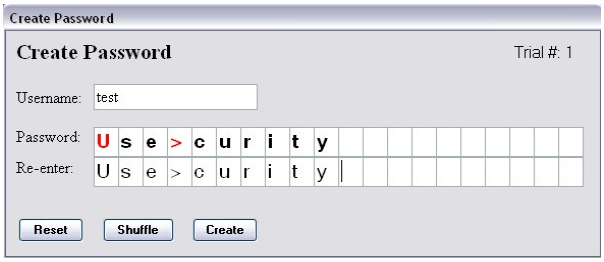


**Figure 4 Persuasive Text Passwords (PTP)**

Even though there are many schemes proposed to improve the password strength, usability studies of these systems tells us, yet another improved schemes need to be introduced. Effective random password choices of users will have high entropy, but will it be memorable? Yan et al. 10 shows that alternative mnemonic phrase-based password scheme is more secure than text passwords, but they are as secure as random passwords. Kuo et al. 10 later discovered that users based their passwords on phrases easily found on the Internet, and as such were no more secure than regular passwords when attacked with a mnemonic dictionary. Alain Forget, Sonia Chiasson, Robert Biddle 10 did a usability study comparing the two mnemonics password schemes and found that users misused both schemes and suggested a new persuasive technology. Memorability of PTP scheme revealed that, it is not effective to users who created secure passwords before the system applied its improvement 1010. Also the persuasive password paper, fail to research whether they defeat against phishing attack.

## 6.2 Password diversity

Password diversity schemes are also called as *password checkers*. Weak passwords are passwords that are easy to guess, or likely to be found in a *dictionary attack*. These schemes are proposed to overcome the *dictionary attack*.

General mechanism of passwords checkers:

- Choose dictionary of unacceptable passwords
- Check whether user chosen password is in the dictionary. If exist reject the password else accept the password

Klein 10 suggests a publicly available proactive password checker, which will enable users to check for the acceptance of the given password against, combination of a dictionary check and other rules to screen for common weak password choices. Spafford 10 describes OPUS, a Bloom filter to compress a dictionary of forbidden passwords. OPUS stores a 250, 000 word dictionary in 350 KB with a 0.5% false positive rate. The OPUS system, as an extra step, adds password choices to the filter. So attempts to re-use old passwords will be refused, hence password aging is supported. A related work uses the OPUS system to gather information on actual user password choices without the risk of leak 10. Manber and Wu 10 describe an approach based on Bloom filters that allows checking both exact and approximate dictionary membership. Therefore, passwords that are a single insertion, deletion, or substitution from a dictionary word will be refused. Bergadano et al. 10 describe a decision tree approach which achieves greater dictionary compression. However, the system does not allow incremental additions of new dictionary words. Instead, retraining must be performed when additions are made 10.

Despite persistent and creative efforts to nudge users toward better practices 10, password strength remains a problem 10. Yan 10 points out that any mismatch between the dictionaries used by the checker and the attacker can resukt in weak passwords being accepted. He suggests augmenting the dictionary checks used in proactive password checking with entropy checks as well. Pinkas and Sander 10 propose the use of CAPTCHA's to slow down dictionary attacks when limiting the number of attempts is undesirable. Van Oorschot and Stubblebine 10 extend this work and show that using login history can greatly reduce the number of CAPTCHA's presented to users.

## 6.3 Password management

Password management schemes are proposed to overcome the phishing attack conducted in the browser to compromise the user password. Note that we didn't consider schemes which discuss about managing multiple text passwords and that is out of our scope. We only consider text password scheme management.

These mechanisms are kind of similar to password checkers. These schemes store username and password of the users in the database, which is encrypted and stored in the most modern browser. Firefox, Safari, Internet Explorer, and Opera store in their browser, where as Mac OS X includes the database in operating system level.

General mechanism of passwords managers:

- Ask user if they want to store their password in the browser.
- If yes, hash and store the password in the browser database.
- When the browser detects that it has returned to a site for which it knows a stored password, it automatically fills in the login form with the stored username and password

Password databases are a component of most modern browsers. These databases do not address the problem of using the same password at multiple sites.

In its relatively short history the problem of phishing has attracted a lot of attention. Dinei Florencio and Cormac Herley 10 have classified and discussed these schemes in detail, but our interest here is to consider the schemes related to the password management, within our scope.

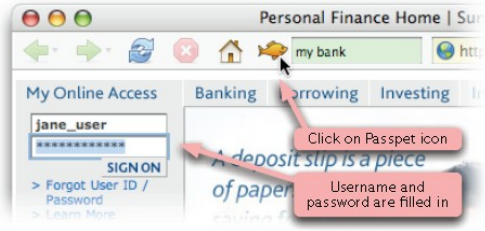


**Figure 5 Passpet**

The idea of domain specific passwords is a very powerful tool in protecting users. Gaber et al. *10* used a master password when a browser session was initiated to access a web proxy, and unique domain specific passwords were used for other web sites. These passwords were hashed using the domain name as a salt. Ross et al. 10 propose a browser extension, PwdHash that uses domain-specific passwords for web sites. Halderman et al. 10 also propose a scheme, Password Multiplier to manage a user's passwords, but this scheme not only protects web passwords but also application passwords from the computer. In contrast to Ross's scheme, hashed passwords are stored in local machine. Kelsey et al. proposed Key Stretching mechanism, which slow hash the password, to avoid brute force attack 10. PassPet (Figure 5) by Yee and Sitaker 10 is also a browser plug-in which manage password. It generates unique passwords for each site and allows automated entry of credentials. WebWallet 10 by Wu et al. warns users if it detects the credentials are being submitted to a non-trusted site.

Usability study of PwdHash and Password Multiplier, by Sonia Chiasson and P.C. van Oorschot 10, shows that simple usability in the mangers leads to security issue, user have inaccurate and incomplete mental model of software, felt that both password manager give great security and they are unwilling to use password managers.

## 6.4 Password theft

Password theft can be in multi form. User tends write down their passwords or share it with friends or others who convince them to do so. Besides social engineering attack, passwords can also be compromised by shoulder surfing attack or key logger attack. Therefore, the schemes discussed here are categorized into schemes which were initially proposed to overcome the shoulder surfing attack, key logger attack and social engineering attack.

### *6.4.1 Shoulder surfing attack*

Shoulder-surfing is an attack on password authentication that has traditionally been hard to defeat. It can be done remotely using binoculars and cameras, using keyboard acoustics.

General mechanism of the schemes:

- Design the user's action or input such that eavesdroppers cannot identify and learn the password

Tan et al. 10 propose a spy-resistant keyboard (Figure 6), which uses a level of indirection to prevent the observer from guessing the password. Their approach adds sufficient ambiguity for the observer to be unable to determine the user's choice without remembering the layout of the entire keyboard. Julie Thorpe et al. proposed more invasive technique, Pass-thought, which extract as much entropy as possible from a user's brain signals upon "transmitting" a thought 10. Manu Kumar et al. 10 proposed EyePassword (Figure 7), which mitigates the issues of shoulder surfing via user gaze as an input.

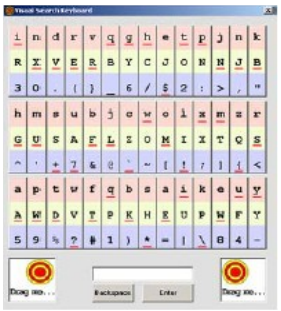

**Figure 6 Spy-resistant keyboard**

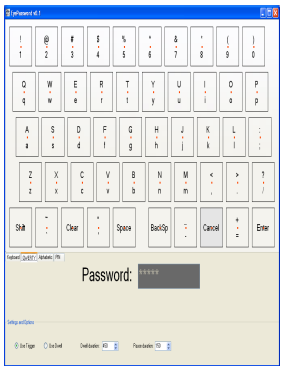


**Figure 7 EyePassword**

Besides, several schemes proposed to defeat the shoulder surfing, Davide Balzarotti 10 shows that if the attacker compromise the surveillance camera near the keyboard, then the text being typed on a keyboard, can be obtain by videoing the user activity.

### *6.4.2 Key logger attack*

Keylogging is one of the most insidious threats to a user's personal information. Unlike Phishing, this is not an attack that alert and sophisticated users can avoid. Key logging tools are commercially available and also it is easy to write.

Home and enterprise users may be able to trust their systems if they maintain good firewall, anti-virus and update strategies. However roaming users have no control over what is installed.

Cormac Herley and Dinei Florencio 10 describe a simple trick the user can employ that is entirely effective in concealing the password from attackers.

### *6.4.3 Social engineering attack*

Social engineering attacks had created growing attention on password security as it compromise the user password, and thus privacy of the user 10. John Brainard et la propose fourth factor authentication, the social network of the user, that is, somebody you know 10 Figure 1. However this topic is out of our scope. Here we propose schemes which were proposed to overcome the social engineering attack in mind.

General mechanism of the schemes:

- Choose a meaningful sentence, easy to remember ad hard to guess
- Use it to authenticate

High entropy passwords are secure, but hard to guess, and hence users write it down. Sigmund N. Porter 10 proposed a very long "pass-phrase" (up to 80 characters), which is hashed (one-way hashing) into the key, and then stored in encrypted form. The hashing necessarily includes one-way encryption. He claims that since the phrase is meaningful to the owner it is easy to remember and resilient to social engineering attack. Passphrases are used to control both access to, and operation of, cryptographic programs and systems, particularly applicable to systems that use the passphrase as an encryption key.

Yishay Spector and Jacob Ginzberg 10 proposed a new methodology based on the conceptual processing of natural language using a pass-sentence. Pass-sentence is based on semantics as well as syntax, as opposed to the syntax-only passwords in use today. They claim that, pass-sentence can significantly hard to guess, more memorable, able to control a level of security and less vulnerable than passwords. They prove they are resilient to social engineering attack, dictionary attach and shoulder surfing attack.

Usability study on pass-phrases conducted by Mark Keith et al. 10 states that, they are resilient to brute force attack, easy to remember but user are unable recall the pass-phrases easily than simple passwords.

## 6.5 Password composition

The security of a password system depends on how difficult it is for a user to determine a valid password. Password composition rules are introduced for users to create a strong password, which is resilient to password vulnerabilities. The composition rules are also called *password policies.*

If we view the password composition policies, it must satisfy the password mechanism goals/elements. Password strength is one of the elements of password mechanism. The numbers of guesses attacker must perform to brute force the correct password and ease with which attacker can check with the dictionary of password, are the two factors which determine the password strength. That is, password strength depends on password length, and complexity.

Here we have chosen papers which discuss password composition rules, tools, user behaviors towards password policy and the security advice.

Password policies are defined by users based on their security needs, standard practice guideline, and resource available, time to time. However there is no strict rule.

Allan's 10 research note:

> "Mitigating authentication weaknesses by increasing password length and complexity will reduce security if passwords are pushed beyond the peak of their effectiveness. They are approaching this point now"

, created an attention over the security community and hence many papers discussed the password policy extensively. Campbell, J. et al. 10 shows enforcement of password composition rules does not discourage users from meaningful information in passwords, and reduce password reuse habit of users. Dinei Florencio et al. 10 report the results of a large scale study of password use and password re-use habits of online users and discuss the detailed data on password strength, types and lengths of passwords chosen, and how they vary by site. Shay, R. et al. 10 defines and models password policies for the entire password policy lifecycle and evaluates the policies using the password simulation tool. Two years later, they published the password simulation tool 10. Referring to last10 years of internet security, Cormac Herley et al 10 quoted that:

> "Despite large numbers of proposed alternatives, we must remember more passwords than ever before. Why is this? Will alphanumeric passwords still be ubiquitous in 2019?"

He stated that, until the direct economic losses become large enough, there may be little incentive to make changes that could lead to problems in support costs or usability. Dinei Florencio and Cormac Herley 10 found that sites with the most restrictive password policies do not have greater security concerns; they are simply better insulated from the consequences of poor usability. R. Shay et al. 10 showed that although most of the users were annoyed by the need to create a complex password, they believe that they are now more secure. Re-examining password policies and password practice in the workplace Philip Inglesant et al. 10 states that password policies should be designed using HCI principles, rather than focusing password policies on maximizing password strength and enforcing frequency alone.

# 7. SECOND GENERATION SCHEMES

Text-based passwords are still the most commonly used authentication mechanism in information systems. Many alternative schemes have been proposed and considerable amount of usability studies have been conducted and some of them proved to be better than text-password scheme both in security and usability. But they failed to replace/dominate the text-passwords to date in practice. Which is the factor that causes the users to rely on them still? This is discussed in Section 8.

We have chosen the schemes which are discussed after this transition and schemes which creates new paradigm in their theory/view as second generation of password schemes.

Second generation of password schemes argue that, not only usability and security is relying on security of the password, but also deployability. Also proposals in this era argue that, there is a

trade off between usability, security and deployability. This is discussed in detail, in *Section 8*.

**Thus, second generation of passwords considered, password security rely on security, usability and deployability of the password and there is a tradeoff between them**.

The schemes we discuss here are categorized based on the goals of the password security mechanisms each category attempts to improve. Here we discussed the goals which have been changed so far.

However, second era has just emerged and therefore few papers have been published to date. Our interest is to show the different views of the new research path and to analyze the transitional changes. We believe this paper will provide comprehensive literature of schemes in both era and hence help the reader to focus on the second generation or the present trend in text password research.

## 7.1 Password composition

Password composition has been made very simple in this era considering the usability of the complex password composition rules.

Serge Egelman et al. 10Error: Reference source not found conducted a survey to experiment the extent to which individuals will tolerate delays when told that such delays are for security purposes. They state that when security mitigations cannot be made free for users, designers may incentivize compliant users' behavior by intentionally drawing attention to the mitigation itself.

Supporting this paper, a scheme has been introduced and is discussed in next section.

## 7.2 Password diversity

Password diversity schemes are proposed to overcome the statistical guessing attacks.

*Statistical guessing attacks* are defined as, a form of *dictionary attack* in which an attacker sorts the password dictionary by presumed, or previously-observed, popularity and guesses the most popular passwords first. To defend against a statistical guessing attack it is important to

- limit the number of guesses that the attacker can issue against each account &
- minimize the cumulative fraction of accounts that use the most popular passwords.

Stuart Schechter et al. 10 propose an oracle to identify undesirably popular passwords using an existing data structure known as a count-min sketch, which they populate with existing users' passwords and update with each new user password. The goal of the *Popularity Oracle* is to achieve only the maximum acceptable rate false-positives, so as to confuse the attacker who tries to copy or query the *Popularity Oracle*.

Mechanism of Popularity Oracle:

- Create a Popularity Oracle of online user passwords. It is still an open question?
- Check the user given password against *Popularity Oracle* to check whether the password is popular.
- If the password exist, then increase the count of the similar password
- If the count value of the password exceeds the threshold value of the Oracle, it asks the user to create a new password. That is less popular password

As the users are encouraged to choose less popular passwords, it is less likely that they are an attractive target to the attacker. User password reuse habit has been extensively discussed in the past history, and it is less likely to affect the current scheme as passwords can be reused in the popularity oracle.

However we don't know anything yet. Security and usability and deployability of this scheme need to be studied in future, to learn about the success of this proposal.

## 7.3 Password strength

Traditional password advice given to users is somewhat dated, and it was argued that strong passwords do nothing to protect online users from password stealing attacks such as *phishing* and *keylogging*, and yet they place considerable burden on users. Weak passwords chosen by users can be compromised. So what can be done to increase the security of the authentication in client side?

Dinei Florencio, Cormac Herley suggested that increasing password strength does little to address any real threat and propose to strengthen the userID's rather than the passwords, if larger credential space is needed 10 .

# 8. TRANSITION

Cormac Herley's 10 argument about security advice, to users:

> "We argue that users' rejection of the security advice they receive is entirely rational from an economic perspective. The advice offers to shield them from the direct costs of attacks, but burdens them with far greater indirect costs in the form of effort."

He pointed that security advice is complex and growing, but the benefit is largely speculative or moot. He concluded that,

> "Users reject security advice as it offers a poor cost-benefit tradeoff to them."

With the failure of the password policies for the composition of passwords, the research community started thinking for appropriate proposals to support this theory. Hence there are very few papers discuss the research open research questions and begin to propose scheme. We will discuss those schemes and idea in out first generation scheme organized format in the next section.

We would like to discuss the papers which induce and knowledge the research community in the new research path.

One of the papers is proposed by Cormac Herley et la.10 . We will discuss his thoughts of "Research Agenda" here.

Among broad authentication research directions to follow, they suggest two broad research directions.

- Identifying scenarios where passwords are indeed the best fit and encouraging means to better support them; this could have tremendous positive impact given the scale of password deployment.
- Systematic prioritizing competing requirements (as rarely can all requirements be met), and using this in comparing alternatives.

Replying to the paper 10 , Joseph Bonneau, Cormac Herley, Paul C. van Oorschot and Frank Stajano 10 proposed a framework by evaluating the two decades of proposals to replace text passwords for general-purpose user authentication on the web. They came up with broad set of twenty-five usability, deployability and security benefits. And they conclude that many academic proposals have failed to gain attraction because researchers rarely consider a sufficiently wide range of real world constraints.

This paper evaluates alternative passwords schemes, compared with text password scheme and derives to the conclusion that more or less some scheme benefit from one factor fails in some other factor. Also this paper didn't survey the text password scheme, but all the other schemes. Text password schemes was not much surveyed recently, but it was surveyed by David L. Jobusch et al. 1010 in 1989. Thus this survey paper will help readers to understand the text password scheme within our scope. However to be complete, challenge response papers and papers discussing PIN passwords can be added to extend this paper.

## 9. SUMMARY

We learnt that most of the schemes are advantage over the other, but none of the scheme is better then simple passwords in deployability. But schemes like persuasive passwords, popularity oracle and pass-sentence gave promising results in security and usability than text passwords. Thus text-password schemes are moving toward producing innovative and promising results to the security research community and most likely to be with for some more time.

## 10. REFERENCES


[1] J. Bonneau, C. Herley, P.C. van Oorschot and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. *IEEE Symp. Security & Privacy 2012*, to appear

[2] R. Morris and K. Thompson, "Password security: a case history," Commun. ACM, vol. 22, no. 11, pp. 594–597, 1979.

[3] A. Adams and M. Sasse, "Users Are Not The Enemy," Commun. ACM, vol. 42, no. 12, pp. 41–46, 1999.

[4] C. Herley and P.C. van Oorschot, "A Research Agenda Acknowleding the Persistence of Passwords," *IEEE Security and Privacy magazine*, Jan. 2012, 28 - 36.

[5] D. Florencio and C. Herley. 2007. A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web* (WWW '07). ACM, New York, NY, USA, 657-666.

[6] S. Gaw and E. W. Felten, "Password Management Strategies for Online Accounts," in ACM SOUPS 2006: Proc. 2nd Symp. on Usable Privacy and Security, pp. 44–55.

[7] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical Passwords: Learning from the First Twelve Years," *ACM Computing Surveys*, vol. 44, no. 4, 2012.

[8] J. Bonneau and S. Preibusch, "The password thicket: technical and market failures in human authentication on the web," in Proc. WEIS 2010, 2010.

[9] D. Florencio and C. Herley, "Where Do Security Policies Come From?", *SOUPS 2010* [Best paper award at SOUPS]

[10] L. Falk, A. Prakash, and K. Borders, "Analyzing websites for user-visible security design flaws," in ACM SOUPS 2008, pp. 117–126.

[11] D. Balzarotti, M. Cova, and G. Vigna, "ClearShot: Eavesdropping on Keyboard Input from Video," in IEEE Symp. Security and Privacy, 2008, pp. 170–183.

[12] B. Kaliski, RFC 2898: PKCS #5: Password-Based Cryptography Specification Version 2.0, IETF, September 2000.

[13] S. Chiasson, P.C. van Oorschot, and R. Biddle. A usability study and critique of two password managers. *In 15th USENIX Security Symposium*, pages 1–16, 2006.

[14] C. Shannon. Prediction and entropy of printed English. In *Bell System Technical Journal*, vol. 30 (1951), pp. 50-64.

[15] *Security and Usability.* Chapter 7 The Memorability and Security of Passwords (J. Yan, A. Blackwell, R. Anderson, and A. Grant)

[16] K. Yee and K. Sitaker. Passpet: Convenient password management and phishing protection. In *Proceedings of the Symposium On Usable Privacy and Security 2006*, Pittsburgh, PA, July 12-14, 2006.

[17] C. Kuo, S. Romanosky, and L. Cranor. Human Selection of Mnemonic Phrase-Based Passwords. In *Proceedings of the Symposium On Usable Privacy and Security 2006*, Pittsburgh, PA, July 12-14, 2006.

[18] A. Forget, S. Chiasson, P.C. van Oorschot, and R. Biddle. 2008. Improving text passwords through persuasion. In *Proceedings of the 4th symposium on Usable privacy and security* (SOUPS '08). ACM, New York, NY, USA, 1-12.

[19] Leonhard, M.D. and Venkatakrishnan, V.N. A Comparative Study of Three Random Password Generators. IEEE EIT 2007, 227-232.

[20] Desney S. Tan , Pedram Keyani , Mary Czerwinski, Spy-resistant keyboard: more secure password entry on public touch screen displays, *Proceedings of the 17th Australia conference on Computer-Human Interaction: Citizens Online: Considerations for Today and the Future*, November 21-25, 2005, Canberra, Australia

[21] Umut Topkara , Mikhail J. Atallah , Mercan Topkara, 2007. Passwords decay, words endure: secure and re-usable multiple password mnemonics. In *Proceedings of the 2007 ACM symposium on Applied computing* (SAC '07). ACM, New York, NY, USA, 292-299.

[22] Julie Thorpe , P. C. van Oorschot , Anil Somayaji, 2005. Pass-thoughts: authenticating with our minds. In *Proceedings of the 2005 workshop on New security paradigms* (NSPW '05). ACM, New York, NY, USA, 45-56.

[23] Min Wu , Robert C. Miller , Greg Little.2006. Web wallet: preventing phishing attacks by revealing user intentions, Proceedings of the *second symposium on Usable privacy and security*(SOUPS ’06), ACM, New York, NY, USA, 102-113.

[24] Alain Forget, Sonia Chiasson, and Robert Biddle. 2007. Helping users create better passwords: is this the right approach?. In *Proceedings of the 3rd symposium on Usable privacy and security* (SOUPS '07). ACM, New York, NY, USA, 151-152

[25] Y. Spector, J. Ginzberg. Pass-sentence a new approach to computer code. *Computers & Security* v.13(1994):145-160.

[26] Mark Keith , Benjamin Shao , Paul John Steinbart, The usability of passphrases for authentication: An empirical field study, *International Journal of Human-Computer Studies*, v.65 n.1, January, 2007, p.17-28.

[27] Eugene H. Spafford, OPUS: preventing weak password choices, Computers and Security, v.11 n.3, p.273-278, May 1992

[28] Campbell, J., Kleeman, D., and Ma, W. 2007. The Good and Not So Good of Enforcing Password Composition Rules. Inf. Sys. Sec. 16, 1 (Jan. 2007), 2-8.

[29] Jeyaraman, S. and Topkara, U. Have the cake and eat it too - Infusing usability into text-password based authentication systems. IEEE ACSAC 2005, 473-482.

[30] C. Herley, "So Long, and No Thanks for the Externalities: the Rational Rejection of Security Advice by Users," In *Proceedings of the 2009 workshop on New security paradigms workshop* (NSPW '09). ACM, New York, NY, USA, 133-144.

[31] S. Schechter, C. Herley and M. Mitzenmacher, "Popularity is Everything: a new approach to protecting passwords from statistical-guessing attacks," In *Proceedings of the 5th USENIX conference on Hot topics in security* (HotSec'10). USENIX Association, Berkeley, CA, USA, 1-8.

[32] D. Florencio, C. Herley and B. Coskun,“Do Strong Web Passwords Accomplish Anything?," In *Proceedings of the 2nd USENIX workshop on Hot topics in security* (HOTSEC'07), Trent Jaeger, Matt Blaze, Angelos D. Keromytis, Patrick McDaniel, Fabian Monrose, Niels Provos, Reiner Sailer, Leendert van Doorn, Helen Wang, and Steve Zdancewic (Eds.). USENIX Association, Berkeley, CA, USA, , Article 10 , 6 pages.

[33] Sonia Chiasson and P.C. van Oorschot. A Usability Study and Critique of Two Password Managers. In *Proceedings of the 15th conference on USENIX Security Symposium - Volume 15* (USENIX-SS'06), Vol. 15. USENIX Association, Berkeley, CA, USA, , pages.

[34] J. Yan, A. Blackwell, R. Anderson, A. Grant. Password memorability and security: empirical results. IEEE Security and Privacy 2(5):25-31, 2004.

[35] S.-T. Sun, Y. Boshmaf, K. Hawkey, K. Beznosov. 2010. A billion keys, but few locks: the crisis of web single sign-on. In *Proceedings of the 2010 workshop on New security paradigms* (NSPW '10). ACM, New York, NY, USA, 61-72.

[36] C. Herley, P. van Oorschot, and A. Patrick. 2009. Passwords: If We're So Smart, Why Are We Still Using Them? In *Financial Cryptography and Data Security*, Roger Dingledine and Philippe Golle (Eds.). Lecture Notes In Computer Science, Vol. 5628. Springer-Verlag, Berlin, Heidelberg 230-237.

[37] K. Renaud. Evaluating authentication mechanisms. In L. Cranor and S. Gar_nkel, editors, Security and Usability: Designing Secure Systems That People Can Use, chapter 6, pages 103{128. O'Reilly Media, 2005.

[38] Sasha Romanosky. 5-899 / 17-500 Usable Privacy and Security Text Passwords, Carnegie Mellon Heinz School, May 2006

[39] R. Housley, T. Polk. Planning for PKI. Wiley, 2001.

[40] L. O’Gorman. Comparing passwords, tokens, and biometrics for user authentication. *Proc. IEEE 91(12):2019-2040,* Dec. 2003.

[41] Mohammad Mannan , P. C. van Oorschot, Digital objects as passwords, Proceedings of *the 3rd conference on Hot topics in security*, p.1-6, July 29, 2008, San Jose, CA

[42] S Egelman, D Molnar, N Christin, A Acquisti, C Herley, S. Krishnamurthi, "Please Continue to Hold: An empirical study on user tolerance of security delays," WEIS 2010

[43] D. Asonov and R. Agrawal. Keyboard Acoustic Emanations In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 3–11, 2004.

[44] L. Zhuang, F. Zhou, and J. Tygar. Keyboard Acoustic Emanations Revisited. In *Proceedings of the ACM Conference on Computer and Communications Security*, pages 373–382, 2005.

[45] Keaton Mowery. UC San Diego. Sarah Meiklejohn. Heat of the moment: characterizing the efficacy of thermal camera-based attacks. *Proceeding of the WOOT'11 Proceedings of the 5th USENIX conference on Offensive technologies*, pages 6-6, 2011

[46] Feldmeier and P. Karn. 1989. UNIX Password Security: Ten Years Later. In *Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology* (CRYPTO '89), Gilles Brassard (Ed.). Springer-Verlag, London, UK, UK, 44-63.

[47] Pinkas, B., and Sander, T. Securing Passwords Against Dictionary Attacks. ACM CCS (2002).

[48] J. Bonneau, The science of guessing: analyzing an anonymized corpus of 70 million passwords, *IEEE Symposium of Security and Privacy*, May 2012.

[49] Dinei Florêncio and Cormac Herley. How To Login From an Internet Café without Worrying about Keyloggers. *Symp. on Usable Privacy and Security*, 2006.

[50] Blake Ross , Collin Jackson , Nick Miyake , Dan Boneh , John C. Mitchell, Stronger password authentication using browser extensions, *Proceedings of the 14th conference on USENIX Security Symposium*July 31-August 05, 2005, Baltimore, MD. p.2-2.

[51] Kumar, M., Garfinkel, T., Boneh, D., and Winograd, T. 2007. Reducing shoulder-surfing by using gaze-based password entry. In Proceedings of the 3rd Symposium on Usable Privacy and Security (Pittsburgh, Pennsylvania, July 18 - 20, 2007). SOUPS '07, vol. 229. ACM, New York, NY, 13-19.

[52] Richard Shay, Abhilasha Bhargav-Spantzel, and Elisa Bertino. 2007. Password policy simulation and analysis. In

*Proceedings of the 2007 ACM workshop on Digital identity management* (DIM '07). ACM, New York, NY, USA, 1-10.

[53] Allan, A. Passwords Are Near the Breaking Point: Gartner Research Note (2004)

[54] Philip G. Inglesant and M. Angela Sasse. 2010. The true cost of unusable password policies: password use in the wild. In *Proceedings of the 28th international conference on Human factors in computing systems* (CHI '10). ACM, New York, NY, USA, 383-392.

[55] Richard Shay and Elisa Bertino. 2009. A comprehensive simulation tool for the analysis of password policies. *Int. J. Inf. Secur.* 8, 4 (August 2009), 275-289.

[56] Richard Shay, Saranga Komanduri, Patrick Gage Kelley, Pedro Giovanni Leon, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2010. Encountering stronger password requirements: user attitudes and behaviors. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (SOUPS '10). ACM, New York, NY, USA, , Article 2 , 20 pages.

[57] Sood, S.K.; Sarje, A.K.; Singh, K. Cryptanalysis of password authentication schemes: Current status and key issues. *In Proceeding of International Conference on Methods and Models in Computer Science*, pp: 1 – 7, 2009.

[58] M. A. Sasse , S. Brostoff , D. Weirich, Transforming the 'Weakest Link' — a Human/Computer Interaction Approach to Usable and Effective Security, BT Technology Journal, v.19 n.3, p.122-131, July 2001

[59] D. V. Klein. Foiling the Cracker: A Survey of, and Improvements to, *Password Security. Proc. of the 2nd USENIX Security Workshop* (1990).

[60] EH Spafford. Observing reusable password choices. Proceedings of the 3rd UNIX Security Symposium (1992).

[61] G. Bergadano, B. Crispo and G. Ruffo. Proactive Password Checking with Decision Trees. Proc. CCS (1997).

[62] U. Manber, S. Wu. An Algorithm for Approximate Membership Checking with Application to Password Security. Information Processing Letters (1994).

[63] J.J. Yan. A Note on Proactive Password Checking. 2001. In *Proceedings of the 2001 workshop on New security paradigms* (NSPW '01). ACM, New York, NY, USA, 127-135.

[64] P.C. van Oorschot, S. Stubblebine. On Countering Online Dictionary Attacks with Login Histories and Humans-in-the-Loop. ACM TISSEC vol.9 issue 3 (2006).

[65] Pinkas, B., and Sander, T. Securing Passwords Against Dictionary Attacks. ACM CCS (2002).

[66] David L. Jobusch and Arthur E. Oldenhoeft. 1989. A survey of password mechanisms: weaknesses and potential improvement, part 1. *Comput. Secur.* 8, 7 (November 1989), 587-601.

[67] D. L. Jobusch and A. E. Oldehoeft. 1989. A survey of password mechanisms: weaknesses and potential improvements. part 2. *Comput. Secur.* 8, 9 (December 1989), 675-689.

[68] Umut Topkara, Mikhail J. Atallah, and Mercan Topkara. 2007. Passwords decay, words endure: secure and re-usable multiple password mnemonics. In *Proceedings of the 2007 ACM symposium on Applied computing* (SAC '07). ACM, New York, NY, USA, 292-299.

[69] Alain Forget and Robert Biddle. 2008. Memorability of persuasive passwords. In *CHI '08 extended abstracts on Human factors in computing systems* (CHI EA '08). ACM, New York, NY, USA, 3759-3764.

[70] Alain Forget, Sonia Chiasson, P. C. Oorschot, and Robert Biddle. 2008. Persuasion for Stronger Passwords: Motivation and Pilot Study. In *Proceedings of the 3rd international conference on Persuasive Technology* (PERSUASIVE '08), Springer-Verlag, Berlin, Heidelberg, 140-150.

[71] Dinei Florencio and Cormac Herley. 2007. Evaluating a trial deployment of password re-use for phishing prevention. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (eCrime '07). ACM, New York, NY, USA, 26-36.

[72] John Brainard, Ari Juels, Ronald L. Rivest, Michael Szydlo, and Moti Yung. 2006. Fourth-factor authentication: somebody you know. In *Proceedings of the 13th ACM conference on Computer and communications security* (CCS '06). ACM, New York, NY, USA, 168-178.

[73] Gregory L. Orgill, Gordon W. Romney, Michael G. Bailey, and Paul M. Orgill. 2004. The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. In *Proceedings of the 5th conference on Information technology education* (CITC5 '04). ACM, New York, NY, USA, 177-181

[74] Sigmund N. Porter. A password extension for improved human factors. *Computers & Security*, Volume 1, Issue 1, January 1982, Pages 54-56

[75] E. Gaber, P. Gibbons, Y. Matyas, and A. Mayer. 199. How to Make Personalized Web Browising Simple, Secure, and Anonymous. In *Proceedings of the First International Conference on Financial Cryptography* (FC '97), Rafael Hirschfeld (Ed.). Springer-Verlag, London, UK, 17-32. Crypto '97.

[76] J. A. Halderman, B. Waters, and E. Felten. 2005. A convenient method for securely managing passwords. In *Proceedings of the 14th international conference on World Wide Web* (WWW '05). ACM, New York, NY, USA, 471-479.

[77] J. Kelsey, B. Schneier, C. Hall, and D. Wagner. Secure applications of low-entropy keys. Lecture Notes in Computer Science, 1396:121-134, 1998.