Security and Usability in Knowledge-based User Authentication: A Review

Christina Katsini
Department of Electrical and Computer Engineering, University of Patras
26504 Rio, Greece
katsinic@upnet.gr

Marios Belk
Department of Computer Science, University of Cyprus
CY-1678 Nicosia, Cyprus
belk@cs.ucy.ac.cy

Christos Fidas
Department of Cultural Heritage Management and New Technologies, University of Patras
26504 Rio, Greece
fidas@upatras.gr

Nikolaos Avouris
Department of Electrical and Computer Engineering, University of Patras
26504 Rio, Greece
avouris@upatras.gr

George Samaras
Department of Computer Science, University of Cyprus
CY-1678 Nicosia, Cyprus
cssamara@cs.ucy.ac.cy

ABSTRACT

This paper presents a comprehensive review of state-of-the-art research works in knowledge-based user authentication, covering the security and usability aspects of the most prominent user authentication schemes; text-, pin- and graphical-based. From the security perspective, we analyze current threats from a user and service provider perspective. Furthermore, based on current practices in authentication policies, we summarize and discuss their security strengths based on widely applied security metrics. From the usability point of view, we present and discuss the usability of each authentication scheme in regards with task performance and user experience. The analysis reveals that although a plethora of alternative user authentication schemes have been proposed in the literature and users interact differently with the various alternatives, online service providers do not yet adopt alternatives to text-based solutions. We further discuss and identify areas for further research and improved methodology with the aim to drive this research towards the design of sustainable, secure and usable authentication approaches.

CCS Concepts

• **Security and privacy → Authentication**

Keywords

Usable Security, Knowledge-based Authentication; Security Metrics; Usability Metrics.

PCI '16, November 10-12, 2016, Patras, Greece
 ISBN 978-1-4503-4789-1/16/11...$15.00
DOI: http://dx.doi.org/10.1145/3003733.3003764

1. INTRODUCTION

With the ever increasing number of services available online, users are required to authenticate themselves many times every day. Numerous authentication mechanisms with different strengths and weaknesses have been proposed and deployed depending on the context of use, which lie under three major categories: *knowledge-based* (e.g., passwords); *token-based* (e.g., credit cards); and *biometric-based* (e.g., fingerprint), and their combinations. Knowledge-based authentication is currently the most common approach for gaining access control in online services [7], with security acting as a contract between the provider and the user, with the provider governing the terms (e.g., deployed authentication policy) and the user having no say. The aforementioned practice raises usability issues due to increased memorizing requirements [19], given that the users find difficulties to remember their passwords and are usually not willing to understand the security issues raised because authentication is a secondary goal for them [13].

Knowledge-based authentication mechanisms include use of a memorized secret for authentication which can be either an alphanumeric password, a personal identification number (PIN) or a graphical secret. Alphanumeric passwords are becoming less usable due to the increasing number of available services that require authentication, combined with strict password policies [16, 19]. Memorability is a major issue leading users in breaking basic security rules such as using very simple passwords, writing them down or reusing the same passwords for different services. Wide use of touch-screen devices has introduced another challenge for alphanumeric passwords, since studies have shown that typing on virtual keyboards is slower and harder than on physical keyboards [33]. To overcome this issue, graphical authentication mechanisms have been proposed. These can be classified under two major categories: the *recall-based* by drawing or identifying locations on an image, and the *recognition-based* by recognizing a set of images among a standard set. Security issues are raised in this case since the authentication key pool is limited compared to alphanumeric passwords [3].

Combinations of the authentication schemes have been proposed and deployed such as credit cards and PINs in ATM machines, and fingerprint embedded in the mobile device (token).

Nonetheless, knowledge-based authentication and more specifically passwords are currently the most common approach for authentication since, in many instances, they are considered the best-fit solution [15]. For example, they don't entail high development and administrative costs as in tokens and biometrics, they don't have security flaws found in tokens (e.g., loss or theft of credit card) and in biometrics (e.g., an individual's fingerprint can be extracted from the objects he touches), they don't have privacy issues of biometrics and they are portable.

In this paper, we review state-of-the-art knowledge-based user authentication mechanisms under two axes: security and usability. For each authentication mechanism we provide a quantification of security based on widely used metrics in the literature with the aim to investigate and compare the strength of each mechanism based on different policies. Regarding usability, we provide a review of existing knowledge-based authentication mechanisms and their usability characteristics. We further discuss the main findings of this analysis and identify areas for further research and improved methodology with the aim to drive this research towards the design of sustainable, secure and usable authentication approaches.

2. SECURITY

2.1 Types of attacks

Security concerns both the users and the service providers for different reasons and using secure authentication mechanisms is of major importance for both, as attackers may be targeting either side. Attacks on the user side lie under the *capture attacks* category, where the goal of the attacker is to steal the authentication key and gain access to the service. These include shoulder surfing, i.e., using observation techniques to get the authentication key; social engineering, i.e., using social manipulation of the user to convince them to divulge confidential information, such as phishing; malware, i.e., using malicious software to gather sensitive information and on touch screen device smudge attacks with attackers aiming to discern the password pattern.

On the other hand, server side attacks which lie under the *guessing attacks* category, where the goal of the attacker is to guess the authentication key by trying guesses repeatedly, the consequences of a successful attack would affect thousands of users and would have an impact on the provider's credibility. Guessing attacks can be further divided in *online guessing* where the attacker interacts directly with the service and *offline guessing* where the attacker has gained access to verifiable text such as cryptographic hashes [14] which can be used to verify guesses. Providers protect the users and the services from online guessing attacks by introducing mechanisms such as CAPTCHA [26], limiting the number of attempts for successful login and delaying the response time after successive incorrect guesses. Offline attacks are harder to deal with since the attacker does not have time limitation other than the computational power of the device used to create the guessed authentication key list. Brute force attack is a widely used offline attack also known as exhaustive key search which entails systematically testing all possible passwords until the correct one is found. For user chosen passwords, search optimizations have been proposed such as dictionary attacks and intelligent brute force [24, 32].

2.2 Security metrics

As discussed previously, users are concerned with capture attacks while providers are mainly concerned with protecting their services from guessing attacks both online and offline. Security is communicated to the users through strict authentication key policies, which ensure the created passwords meet a minimum security level. There are a number of security metrics that enable the comparison between the different authentication policies such as password strength, guessability and entropy.

Focusing on knowledge-based authentication keys, *guess numbers*, *password strength meters* and *entropy* are three common approaches for measuring the security level. Guess numbers refer to how many guesses it would take for a cracking algorithm with a given training set up to guess a password [34]. This approach refers to parameterized password guessability which aims to model real-world attackers and provide strength estimates per password. Despite recent research favouring guessability and guess numbers as a new more modern and accurate metric for measuring security [11, 12, 18, 20, 31], their effectiveness depends on the selected algorithm and on the training data. Its value lies in providing a per password estimation meaning it can be used for security audits and for providing feedback when creating passwords, through strength meters.

A password strength meter refers to checking the created password against a set of rules before submitting it to the system and providing feedback to the user through a word qualifying password strength (e.g., weak, medium, strong, very strong). The accuracy of many deployed password checkers is low because they are often too simple to capture the complexity of passwords [6, 11]. Combining this with the fact that password distribution may be significantly different for different sites (e.g., due to language differences), means there is no global password checker available that can be applied to all Web-sites. However, password strength meters allow for quickly checking the created password for patterns (e.g., dictionary words, repeats or sequences) and some providers restrict the use of such patterns while others only inform the users for the strength of the selected password.

The metrics discussed so far refer to per-password security. Entropy is a security metric per policy. Shannon introduced entropy as a measure of uncertainty of choices [29]. In terms of authentication, entropy refers to how random users select passwords from a given key space, relates to how difficult attackers can guess a password [5] and is enforced through a password policy. The password key space (K_p) refers to the range of all possible values of key combinations and is governed by the character pool and the key length. Entropy is measured in bits and is calculated using the following equation [25]:

$$H_{max} = log_2 K_p \, [bits]$$

Users tend to select memorable passwords rather than random. This password selection strategy results in a non-uniform distribution of the key space, making the entropy lower or even vanish. To describe this phenomenon, researchers distinguish between the aforementioned theoretical entropy and the practical entropy which stands for the entropy resulting from the non-random selection of passwords by users. The practical entropy is difficult to measure, mainly due to users' being sceptical in disclosing information regarding their password creation strategy and the inability of accessing raw password data. To confront this problem, providers have introduced dictionary checks, where common words and character combinations are not allowed to be used as passwords. The NIST Electronic Authentication Guideline SP-800-63 allows for calculating and estimate practical entropy based on Shannon's estimation of the entropy of each successive character of the English alphabet [5]. To this end, the discussed metrics and research work have been mostly applied in text-based

Table 1. Summary of security aspects of knowledge-based authentication mechanisms

U: upper-case letter, N: number, S: symbol. For Dictionary checks 0: no check, 1: check without preventing key creation, and 2: check preventing password creation

Providers/ Schemes		Min Length	Character Pool	Required Charset	Theoretical Entropy	Dictionary Check	Guess-ability	Strength Meter	Estimated Practical Entropy
Text-based AM of Worldwide Large Service Providers	Google	8	94	ø	52.44 bits	2	yes	Too short, Weak, Good, Strong	24 bits
	Facebook	6	94	ø	39.33 bits	0	no	Weak, Medium, Strong	14 bits
	Yahoo	9	94	ø	58.99 bits	0	yes	no	25.5 bits
	Twitter	6	94	ø	39.33 bits	0	no	Too short, Too obvious, Weak, Good, Strong, Very Strong	14 bits
	Live	8	94	At least two of U, N, S	52.44 bits	0	yes	no	30 bits
	Instagram, Amazon, Ebay	6	94	ø	39.33 bits	0	no	no	14 bits
	Booking	8	94	ø	52.44 bits	0	no	no	18 bits
	Linkedin	6	94	ø	39.33 bits	1	no	2-5	14 bits
	Dropbox	6	94	ø	39.33 bits	1	yes	Weak, So-so, Good, Great	20 bits
PIN based AM	PIN	4	10	ø	13.29 bits	no	no	no	9 bits
Graphical AM	Pattern	4	9	n/a	11.56 bits	no	no	no	n/a
	Image Pass [21]	5	25	n/a	22.58 bits	no	no	no	n/a
	PassFaces [4]	4	36 (4x9 image grid)	n/a	12.69 bits	no	no	no	n/a
	VIP 10 [10] VIP 16 [10]	4 4	10 16	n/a n/a	12.30 bits 15.41 bits	no no	no no	no no	n/a n/a
	GesturePuzzle [29]	4	30	n/a	19.63 bits	no	no	no	n/a

authentication mechanisms. Nonetheless, the aforementioned metrics can be applied to graphical authentication mechanisms with minor adjustments. Rass et al. proposed a methodology for calculating the theoretical entropy for a graphical authentication mechanism based on unordered image selection from a given pool [27]. It should be noted that when using images instead of text, random selection of authentication keys becomes more viable [28]. Kayem provides a comparison of the vulnerability to guessing between text-based authentication keys and recall-based graphical authentications keys and suggests that the latter outperform in terms of security [17]. Davis et al., conducted a large scale empirical study on user choices in graphical authentication mechanisms and concluded that user choices are far from random and depend on gender and race [9], which suggests that a strength meter could also serve as a security metric for graphical authentication schemes just as for passwords.

2.3 Security analysis

In Table 1 we summarise and compare the authentication policies used by some of the worldwide largest service providers and some graphical authentication mechanisms introduced in research. We provide the character length, the character pool size and we have calculated the theoretical entropy for these mechanisms. For the text-based password policies we also provide the estimated practical entropy calculated using the NIST guidelines [5]. Dictionary checks, strength meters and guessability refer to whether the provider is using these metrics.

Password lengths vary between a minimum of six and eight characters, with Yahoo being the only large provider that requires a nine character long password. Additional requirements such as use of special characters, numbers and/or upper-case letters are only imposed by Live's password policy. A difference of two characters in password length results in a theoretical entropy difference of approximately 13 bits; a severe degradation on security. To overcome this security issue some of the providers have introduced password meters, ranging between three to six level likert-type scales and in cases where the created password is very weak, they prevent password creation. Four digit PIN-based authentication mechanisms have a theoretical entropy of 13.29 bits and are always used in combination with token-based mechanisms. Most often, additional security is achieved by locking the token after three failed attempts to enter the PIN. For the recognition-based graphical authentication mechanisms the length of the password is usually limited to four or five images and the character pool is between ten and thirty six characters, which is much lower than the ninety four characters of the

password based. Entropy lies between 12.30 and 22.58, which again is much lower when compared to that of the password basedmechanisms described previously. No dictionary checks, strength meters or gueassability mechanisms have been developed for graphical based passwords despite that research has proven that people create predictable graphical based passwords [9,22].

3. USABILITY

A number of research works have investigated the usability of various knowledge-based authentication schemes. The most prominent usability dimensions being measured are task efficiency (e.g., time to register and time to login), task effectiveness (e.g., number of attempts to login) and user preference (e.g., whether the user prefers a particular authentication schemes over another). Recently, research has also focused on studying the influence of contextual factors (human and technology specific) towards the usability of user authentication, by investigating the effects of age differences [23], cognitive styles and abilities [1, 2, 20], device characteristics (e.g., device type, interaction design and virtual keyboard layout) [30, 33], etc., towards task performance and user experience of various user authentication schemes.

An early study of Brostoff and Sasse [4] has investigated the usability of traditional password schemes and graphical authentication (Passfaces). Results of the study have shown that overall, graphical authentication needs more time to complete, however on the contrary graphical authentication has higher success rate compared to text-based and users authenticate less frequently on graphical authentication than text-based passwords. In Wiedenbeck et al. [35], a longitudinal study was run aiming to investigate the usability of traditional passwords and a new graphical authentication scheme (PassPoints). Results have shown that users created the graphical key faster and with less difficulties than the password key during system registration. However, login times and failed attempts with the graphical authentication scheme were higher than the password scheme.

Nicholson et al. [23] studied the effect of age (young vs. older adults) on the task effectiveness (number of attempts to authenticate) of PIN-based and graphical authentication schemes. Results have shown an effect of age on task effectiveness, with young adults requiring less attempts to authenticate than older adults on both authentication schemes. A comparison between PIN-based and graphical authentication within each user group further revealed that young adults required a similar number of attempts to authenticate, whereas older adults required more attempts in the PIN-based schemes compared to the graphical.

Belk et al. [2] recently investigated whether human cognitive differences in information processing affect task completion efficiency and effectiveness among text-based and graphical authentication schemes. Results have shown that overall, users complete the traditional text-based task faster than the graphical task. Furthermore, cognitive differences (Verbals vs. Imagers) have shown a main effect on task completion time, with Verbals completing the text-based task faster than Imagers, whereas Imagers completing the graphical task faster than Verbals. Within a similar context, Ma et al. [20] studied how cognitive disabilities (Down syndrome vs. neuro-typical) affect task performance and user preference in traditional text-based and graphical authentication schemes. Similarly, results show that among both user groups, text-based tasks are completed more efficiently and effectively than graphical tasks. In addition, individuals with Down syndrome require more time to register and login using a text-based password scheme than neuro-typical individuals.

From the technology point of view, with the advent of new interaction devices (e.g., touch interaction with tablets, smart phones, wearables, etc.), researchers have investigated how several technology factors affect user authentication task performance. For example, von Zezschwitz et al. [33] compared password completion performance and password key choice among various device types (desktop computers, tablets, smartphones). Results showed that entering passwords on a virtual keyboard on tablet and smartphone devices is slower compared to traditional keyboards on desktop computers, and users tend to choose easy and fast to enter passwords on mobile devices. Schlöglhofer et al. [30] compared the time to unlock a smartphone device through PINs, text-based passwords and graphical authentication schemes suggesting that PINs are the fastest to enter, graphical authentication is considered as usable as PINs and passwords are the least usable.

4. DISCUSSION

The paper presented a review of state-of-the-art research works in knowledge-based user authentication (text-, pin- and graphical-based) in an effort to better understand the security and usability aspects of these schemes. In this respect, we have analyzed and summarized the security and usability aspects of the presented user authentication schemes based on widely applied security and usability metrics found in the literature. The analysis presented in this paper further supports that Usability in user authentication is affected by contextual factors (human, technology, design) and that there is a Security gap between text-based and graphical authentication mechanisms.

Usability in user authentication is affected by contextual factors (human, technology, design): Existing studies in knowledge-based user authentication reveal that human, technology and design factors affect usability in user authentication. These findings underpin the necessity of adaptivity in user authentication design; the need of schemes that intelligently adapt to the unique characteristics of each user, the interaction device and the overall context of use. Nonetheless, as shown in the security analysis, high profile service providers still follow a *"one-size-fits-all"* paradigm; the same password scheme is deployed neglecting the fact that users have diverse characteristics that affect differently the usability of the task.

Security gap between text-based and graphical authentication mechanisms: The increasing number of services available online requires users to authenticate multiple times per day. Moreover, as stated previously, users authenticate nowadays through a variety of interaction devices and behave differently with regards to preference and performance. In this context, despite research indicating that, under specific contexts of use, graphical authentication mechanisms outperform text-based in terms of task efficiency and effectiveness, and user preference, online service providers (like Google, Yahoo, etc.) provide no alternative other than text-based, regardless of the type of the device used, the age and the abilities (physically or cognitive) of the users. This is mainly due to the reduced security of the proposed graphical mechanisms, based on the theoretical entropy which is much lower when compared to that of the most widely deployed policies for text-based mechanisms, as shown in Table 1. This difference in the entropy constitutes graphical authentication mechanisms more susceptible to guessing attacks. Security wise, as there are several mechanisms for confronting online guessing attacks, the main concern of the providers lies in the offline guessing attacks, discussed in Section 2.1.

Table 2. Factors affecting the user experience in knowledge-based user authentication.

L: lower-case letter, U: upper-case letter, N: number, S: symbol, Reg: Registration time; Log: Login time; Eff: Effectiveness

Source	Human	Technology	User Groups	Security Policy	Password			PIN			Graphical		
					Reg	Log	Eff.	Reg	Log	Eff.	Reg	Log	Eff.
[20]	Cognitive disability	Desktop	Down syndrome Neuro-typical	*Password:* Len: 2-20 (N, U, S) *Graphical:* Len: 3 K_p: 30	247s 83s	45s 14s	-	-	-	-	-	58s 22s	-
[23]	Age	Desktop	Young adults Older adults	*PIN:* Len: 4 (N) *Passfaces:* 4 images x 4 9-image grid	-	-	-	-	-	3.6/5 2/5	-	-	4.8/5 3.6/5
[2]	Cognitive styles	Desktop	Verbal Imager	*Password:* Len: min 8 (N, U, S) *Graphical:* 8-12/16 images	35s 36s	12s 14s	*Success* 87% 85%	-	-	-	87s 79s	14.5s 13s	*Success* 80% 91%
[33]	-	Different devices	Desktop Smartphone Tablet	*Random password:* Len: 8 (2L, 2U, 2N, 2S)	-	7.5s 13.2s 12.8s	*Failure* 28.6% 47.6% 23.8%	-	-	-	-	-	-
[30]	-	Smartphone	Smartphone	n/a	-	10s	-	4s	-	-	-	-	-
[8]	-	Desktop	-	*Graphical:* 4 images in 4x9-grid screens	-	-	-	-	-	-	70.6s	18.2s	80%
[35]	-	Desktop	-	*Password:* Len: 8 (N, U, S) *Graphical:* 5 points / 373: K_p: $7.2x10^{12}$	81s	9.2s	*Attempt* 1.7	-	-	-	64s	19.3s	*Attempt* 1.5
[4]	-	Desktop	-	*Password:* Len: 8 (N, U, S) *Graphical:* Len: 4 K_p: 36	16.3s	-	*Failure* 33.91	-	-	-	20s	-	*Failure* 12.3

5. CONCLUSION AND FUTURE WORK

To conclude, we stress that research in usable security for knowledge-based user authentication schemes is still trying to find a viable compromise between usability and security. This is mainly because service providers' concerns and priorities are primarily related to security aspects whereas users on the opposite request a more viable equilibrium between security and usability. Several studies, in the field of knowledge-based user authentication mechanisms, suggest that graphical authentication mechanisms outperform the text-based in terms of usability but on the other hand come short in terms of security. Thus, alternatives are not currently adopted by online service providers since they fail to reach a desired level of security. Hence, in practice only text-based mechanisms are nowadays deployed in online services regardless of the context of use. Furthermore, service providers increase continuously the security levels by introducing strict policies in order to ensure a minimum required level of security.

The advent of ubiquitous computing and pervasive systems impose the use of different devices in different contexts. In that context, natural interfaces are not far from intruding our everyday lives and they will bring new challenges but also new opportunities in user authentication which will be worth investigating.

6. REFERENCES

[1] Belk, M., Germanakos, P., Fidas, C., & Samaras, G. 2013. Studying the effect of human cognition on user authentication tasks. In *International Conference on User Modeling, Adaptation, and Personalization*. Springer Berlin Heidelberg, 102-113.

[2] Belk, M., Fidas, C., Germanakos, P., & Samaras, G. 2015. Do human cognitive differences in information processing affect preference and performance of CAPTCHA?. *International Journal of Human-Computer Studies*, *84*, 1-18.

[3] Biddle, R., Chiasson, S., & van Oorschot, P. 2012. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys,* 44(4), 41 pages.

[4] Brostoff, S., & Sasse, M. A. 2000. Are Passfaces more usable than passwords? A field trial investigation. In *People and Computers XIV—Usability or Else!*, Springer, 405-424.

[5] Burr, W. E., Dodson, D. F., & Polk, W. T. 2004. *Electronic authentication guideline*, 800-63. US Department of Commerce, Technology Administration, National Institute of Standards and Technology.

[6] Castelluccia, C., Dürmuth, M., & Perito, D. 2012. Adaptive Password-Strength Meters from Markov Models. In *Network and Distributed System Security Symposium (NDSS 2014)*.

[7] Chiasson, S., Forget, A., Stobert, E., van Oorschot, P. C., and Biddle, R.. 2009. Multiple password interference in text passwords and click-based graphical passwords. In *Procs of the 16th ACM conference on Computer and communications security* (CCS '09). ACM, New York, NY, USA, 500-511.

[8] Chowdhury, S., Poet, R., & Mackenzie, L. 2013. A comprehensive study of the usability of multiple graphical passwords. In *IFIP Conference on Human-Computer Interaction*. Springer Berlin Heidelberg, 424-441.

[9] Davis, D., Monrose, F., & Reiter, M. K. 2004. On User Choice in Graphical Password Schemes. In *USENIX Security Symposium.* Vol. 13, 11-11.

[10] De Angeli, A., Coventry, L., Johnson, G., & Renaud, K. 2005. Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. *Journal of Human-Computer Studies*, *63*(1), 128-152.

[11] De Carné de Carnavalet, X., and Mannan, M. 2014. From very weak to very strong: Analyzing password-strength meters. In *Network and Distributed System Security Symposium (NDSS 2014)*.

[12] Dürmuth, M., Angelstorf, F., Castelluccia, C., Perito, D., & Chaabane, A. 2015. OMEN: Faster password guessing using an ordered markov enumerator. In *International Symposium on Engineering Secure Software and Systems* (Mar 2015) Springer International Publishing, 19-132.

[13] Fidas, C. A., Voyiatzis, A. G., & Avouris, N. M. 2010. When security meets usability: A user-centric approach on a crossroads priority problem. In *Informatics (PCI), 2010 14th Panhellenic Conference* IEEE, 112-117.

[14] Gong, L., Lomas, M. A., Needham, R. M., & Saltzer, J. H. 1993. Protecting poorly chosen secrets from guessing attacks. *IEEE journal on Selected Areas in Communications*, *11*(5), 648-656.

[15] Herley, C., & Van Oorschot, P. 2012. A research agenda acknowledging the persistence of passwords. *IEEE Security & Privacy*, *10*(1), 28-36.

[16] Inglesant, P. J. and Sasse, M. A. 2010. The true cost of unusable password policies: password use in the wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '10). ACM, NY, USA, 383-392.

[17] Kayem, A. V. 2016. Graphical Passwords-A Discussion. *30th International Conference on Advanced Information Networking and Applications Workshops.* IEEE, 596 – 600.

[18] Kelley, P. G., Komanduri, S., Mazurek, M. L., Shay, R., Vidas, T., Bauer, L., and Lopez, J. 2012. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In *2012 IEEE Symposium on Security and Privacy* (May, 2012) 523-537.

[19] Komanduri, S., Shay, R., Kelley, P.G., Mazurek M. L., Bauer, L., Christin, N., Cranor L. F., and Egelman, S. 2011. Of passwords and people: measuring the effect of password-composition policies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '11). ACM, New York, NY, USA, 2595-2604.

[20] Ma, J., Yang, W., Luo, M., & Li, N. 2014. A study of probabilistic password models. In *2014 IEEE Symposium on Security and Privacy* (May 2014) 689-704.

[21] Mihajlov, M., & Jerman-Blažič, B. 2011. On designing usable and secure recognition-based graphical authentication mechanisms. *Interacting with Computers*, *23*(6), 582-593.

[22] Mihajlov, M., Jerman-Blažič, B., & Shuleska, A. C. 2016. Why That Picture? Discovering Password Properties in Recognition-based Graphical Authentication. *International Journal of Human–Computer Interaction*, (just-accepted).

[23] Nicholson, J., Coventry, L., & Briggs, P. 2013. Age-related performance issues for PIN and face-based authentication systems. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 323-332.

[24] Oechslin, P. 2003. Making a faster cryptanalytic time-memory trade-off. In *Annual International Cryptology Conference* Springer Berlin Heidelberg, 617-630.

[25] O'Gorman, L. 2003. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, *91*(12), 2021-2040.

[26] Pinkas, P., and Sander, T . 2002. Securing passwords against dictionary attacks. In *Proceedings of the 9th ACM conference on Computer and communications security* (CCS '02), Vijay Atluri (Ed.). ACM, NY, USA, 161-170.

[27] Rass, S., Schuller, D., & Kollmitzer, C. 2010. Entropy of graphical passwords: towards an information-theoretic analysis of face-recognition based authentication. In *IFIP International Conference on Communications and Multimedia Security* Springer Berlin Heidelberg, 166-177.

[28] Shepard, R. N. 1967. Recognition memory for words, sentences, and pictures. *Journal of verbal Learning and verbal Behavior*, *6*(1), 156-163.

[29] Shannon, C. E. 2001. A mathematical theory of communication. *SIGMOBILE Mob. Comput. Commun. Rev.* 5, 1 (Jan 2001), 3-55.

[30] Schlöglhofer, R., & Sametinger, J. 2012. Secure and usable authentication on mobile devices. In *Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia*. ACM, 257-262.

[31] Ur, B., Segreti, S. M., Bauer, L., Christin, N., Cranor, L. F., Komanduri, S., & Shay, R. 2015. Measuring real-world accuracies and biases in modeling password guessability. In *USENIX Security Symposium (Security 15)*. 463-481.

[32] Van Oorschot, P. C., & Wan, T. 2009. TwoStep: An authentication method combining text and graphical passwords. In *International Conference on E-Technologies* Springer Berlin Heidelberg, 233-239

[33] Von Zezschwitz, E., De Luca, A., and Hussmann, H. 2014. Honey, I shrunk the keys: influences of mobile devices on password composition and authentication performance. In *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational* (NordiCHI '14). ACM, New York, NY, USA, 461-470.

[34] Weir, M., Aggarwal, S., Collins, M., and Stern, H. 2010. Testing metrics for password creation policies by attacking large sets of revealed passwords. In *Proceedings of the 17th ACM conference on Computer and communications security* (CCS '10). ACM, New York, NY, USA, 162-175.

[35] Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., & Memon, N. 2005. PassPoints: design and longitudinal evaluation of a graphical password system. *Int. J. Hum.-Comput. Stud.* 63, 1-2, 102-127.