FlexPass: Symbiosis of Seamless User Authentication Schemes in IoT

Marios Belk
School of Sciences, University of Central Lancashire, Cyprus Campus, 7080 Larnaka, Cyprus
mbelk1@uclan.ac.uk

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

Andreas Pitsillides
Department of Computer Science, University of Cyprus, 1678 Nicosia, Cyprus
andreas.pitsillides@ucy.ac.cy

ABSTRACT

This paper presents a new user authentication paradigm which is based on a flexible user authentication method, namely *FlexPass*. FlexPass relies on a single, user-selected secret that can be reflected in both textual and graphical authentication secrets. Such an approach facilitates adaptability in nowadays ubiquitous user interaction contexts within the Internet of Things (IoT), in which end-users authenticate multiple times per day through a variety of interaction device types. We present an initial evaluation of the new authentication method based on an in-lab experiment with 32 participants. Analysis of results reveal that the FlexPass paradigm is memorable and that users like the adaptable perspective of the new approach. Findings are expected to scaffold the design of more user-centric knowledge-based authentication mechanisms within nowadays ubiquitous computation realms.

CHI'19 Extended Abstracts, May 4–9, 2019, Glasgow, Scotland UK

ACM ISBN 978-1-4503-5971-9/19/05.
https://doi.org/10.1145/3290607.3312951

KEYWORDS

Internet of Things; Knowledge-based User Authentication; Textual Passwords; Graphical Passwords; Feasibility Study.

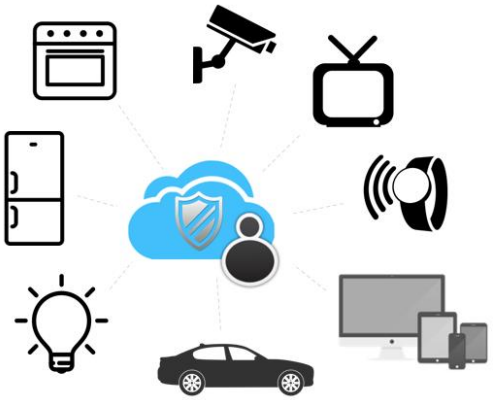

Figure 1: Users authenticate themselves in numerous IoT-enabled devices.

1 INTRODUCTION

The rise of mobile and wearable computing, and the increasing advancements of connected Internet of Things (IoT) has created new opportunities and challenges for security and privacy. Recent research in IoT security and privacy has focused on software engineering security practices [1, 2], patching networked devices [3], access control policy specification, and redesigning IoT-based authentication for sharing passwords among multiple users for unlocking devices [4, 5].

In this realm, user authentication is a critical security task in IoT performed by millions of individuals daily to access their computers, smartphones, smart TV and smart home applications (**Figure 1**). To date, alphanumeric or pin-based passwords are the most common solution for authentication in IoT [4]. However, empirical studies report that current password policies lead often to frustration (when users forget their password, or having a hard time remembering it due to increased complexity of password policies) [6]; security breaches (when users create predictable passwords or write down their passwords) [7]; and operational expenses (when users request new password keys that have been forgotten or lost) [8]. In addition, with the advent of touch-based surfaces and hand-gesture-based modalities in IoT, traditional passwords inherit device-specific interaction difficulties [9, 10] and thus seem not to be adequate for task execution performance.

In this respect, researchers have attempted to provide an alternative to textual passwords by proposing graphical password systems which ask users to complete an image-based task to login. Graphical passwords have shown to have good usability and security characteristics [2] and are now being widely adopted, *e.g.*, Windows 10 picture password. Many graphical password systems have been proposed (see [7] for a review) which either require users to sketch a secret image or pattern on the screen [11, 12], or select and recognize pictures on a grid [13], or provide users with various cues (visual, verbal, and spatial) to assist the recognition of system-assigned keywords [19].

Research Motivation. From an end-user perspective, evidence has shown that user preference and task performance in textual and graphical passwords vary significantly depending on the user and the context of use, suggesting that any specific solution might not please everyone [14]. In particular, research has shown that users with different age [15], cognitive disabilities [16], cognitive abilities [17] prefer and perform differently in textual and graphical passwords. From the technology perspective, studies indicate that the device type, such as touch screens, hand gestures, etc. affect the users' performance and behavior in textual and graphical passwords [9].

Thus, bearing in mind that: *a)* users prefer and perform differently on textual and graphical passwords; and *b)* nowadays user authentication in IoT is performed on multiple heterogeneous devices, this paper investigates whether end-users would benefit from an adaptable user authentication solution that allows users to choose between different authentication types depending on their context of interaction, while preserving security. Our work is primarily driven by our vision to combine textual and graphical password schemes based on a new flexible user authentication paradigm, coined *FlexPass*, which allows us to move from current generic "one-size-fits-all" authentication systems to flexible, user-adaptable authentication systems.

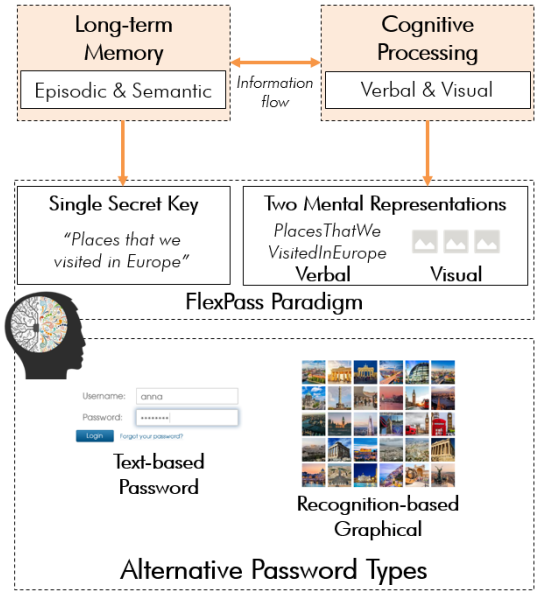

Figure 2: The FlexPass concept. Consider a password creation scenario in which a user chooses a secret derived from his episodic memory, *e.g.*, *"Places that we visited in Europe"*. In this scenario, the textual password key is based on the articulation of the secret, *e.g.*, the system will generate a textual password key *"PlacesThatWeVisitedInEurope"*. For the creation of the graphical password key, the user chooses pictures illustrating relevant images through search in Web engines. Other related images from the image search default to decoy images. Both user-selected and decoy images are finally assigned to the user's profile to be used for login.

2 FLEXIBLE USER AUTHENTICATION PARADIGM

2.1 Theoretical Background and FlexPass Concept

FlexPass aims to leverage on two known theories from cognitive sciences which relate to human information processing and storage; the *Dual Coding Theory*, and *Episodic and Semantic Memory*.

Dual Coding Theory. The dual coding theory suggests that visual and verbal information is processed and represented differently along two distinct cognitive sub-systems in the human mind; the *visual* and the *verbal cognitive sub-systems*. Each sub-system creates separate visual and verbal representations for information being processed which are stored in two independent memory systems; a *verbal* and an *image memory*. Both types of representations can be used when recalling information [18]. For example, the concept "human" is mentally represented as both the word "human" and as the image of a human. When recalling that concept, the individual can retrieve either the word or the image individually, or both simultaneously.

Episodic and Semantic Memory. According to the Atkinson-Shiffrin memory model [27], long-term memory is the final stage of memory in which information (*e.g.*, a secret password key) remains for a long period of time or indefinitely. Long-term memory consists of episodic and semantic memory. *Episodic memory* [20] involves the recollection of personal experiences in events and certain situations (*e.g.*, memories of a family trip in Europe), whereas *semantic memory* [21] involves storage of factual information about the world that people have collected in life (*e.g.*, facts, ideas, meaning and concepts). Combinations of episodic and semantic memory can form autobiographical memory which consists of episodes recollected throughout life and semantic knowledge about the world [22]. Information in both episodic and semantic memory can be stored for a long period [23].

FlexPass attempts to provide a new user authentication paradigm that leverages upon the aforementioned theories, which suggest that humans' episodic and semantic memories, represented as verbal and visual information, can be transformed into memorable and personal authentication secrets. Such secrets can be semantically similarly reflected on both textual and graphical password keys, and accordingly used complimentary based on user preference (**Figure 2**). The FlexPass paradigm relies on a single, open-ended, user-selected secret that can be reflected as a textual key and a graphical key. The paradigm has been realized as two main processes: *i)* creation of the single secret and its two reflections; and *ii)* user-adaptable authentication.

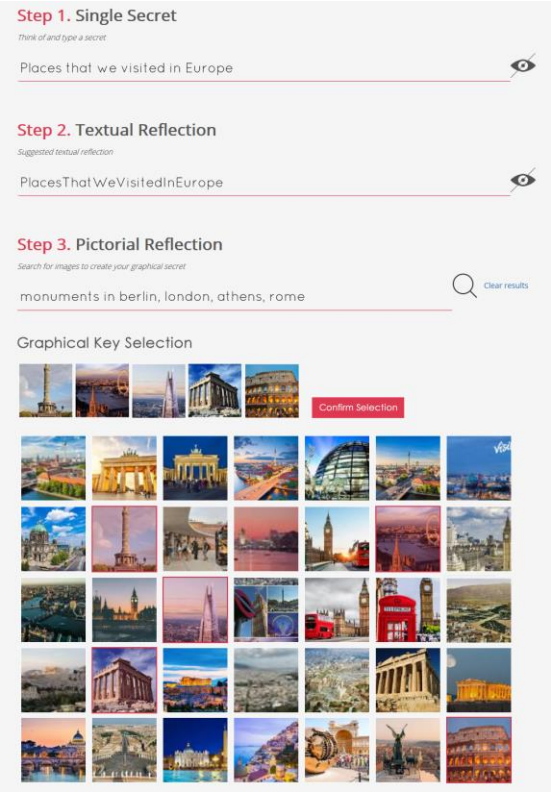

Figure 3: User enrolment/registration of the FlexPass prototype. In this scenario, the user performs a query in which images are asynchronously retrieved from Google Images using the Google Custom Search API.

3 PROTOTYPE IMPLEMENTATION

3.1 Creation of the Single Secret and its Two Reflections

The user enrolment/registration phase is split in three main steps (**Figure 3**): *i)* users choose and type a single secret they wish, *e.g.*, *"Places that we visited in Europe"*; *ii)* the system generates a textual password key based on the single secret, *e.g.*, *"PlacesThatWeVisitedInEurope"*, in which users are free to slightly modify the text, *e.g.*, change upper- to lower-case letters, include special characters, etc.; and *iii)* users create a recognition-based graphical password key. We intentionally chose at this stage to use recognition graphical passwords since research has shown that these are the most memorable among existing graphical password systems (*vs.* pure recall- and cued-recall-based) [24], and because secret concepts can be semantically reflected through a set of images.

3.2 Flexible Authentication in IoT Interaction Realms

During user authentication, users can choose their preferred way to authenticate; either by entering the textual key or the graphical key. **Figure 4** illustrates a login scenario in which the user selected a textual password as his preferred way to login. In each login session, the alternative option (*e.g.*, graphical password) is available to switch based on the user's preference. Entering the textual key follows the same process as traditional passwords. For entering the graphical key, a 7x7 grid containing the user-selected and system-generated decoy images are presented. The image positions in the selection grid are randomly positioned in each login session. Thereafter, users have to select their images in the specific sequence, as entered in the enrolment phase to login.

Usage Scenario. Users interacting with a touch-based IoT device might prefer to login with a graphical password, instead of entering text on a virtual keyboard which is considered a demanding and time-consuming task [9, 10]. The same user however, in a different context, *e.g.*, working on the desktop computer, can choose to login through his textual password key. Note that in both cases, the user is only required to recall the same single secret, which can be reflected differently based on the user's preference. Furthermore, since user authentication in IoT is shifting from single-user passwords towards shared passwords, users sharing the same secret, *e.g.*, older adults, might prefer to login with a graphical password than younger adults of the family [15].

3.3 Security Considerations and Password Creation Policies

FlexPass follows state-of-the-art security metrics and authentication policies [7, 25, 26]. The textual password keys rely on a basic 16-character password policy, allowing the creation of dictionary words with no composition requirements which is more usable and as secure as traditional complex 8-character policies [25] (NIST predicts that both policies generate 30 bits of security entropy [26]). The graphical keys rely on a 5-image policy out of a 7x7 image grid which generates 21 bits of security entropy ($log_2\binom{7\times 7}{5}$). We chose this policy as a guideline by following well-cited works that consider this entropy as sufficient for everyday computing [24]. Online guessing attacks are prevented in both authentication systems through Human Interaction Proofs (*e.g.*, captcha) that are enabled after three unsuccessful user logins.

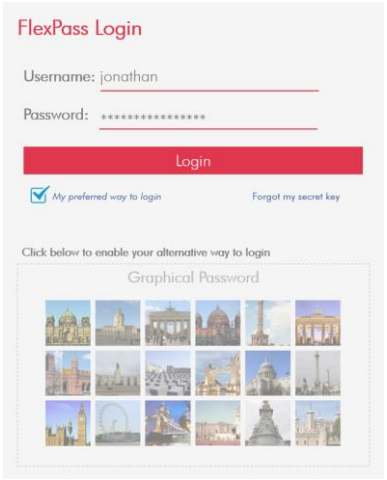

Figure 4: User-adaptable authentication in which the user can choose between the textual and graphical mechanism.

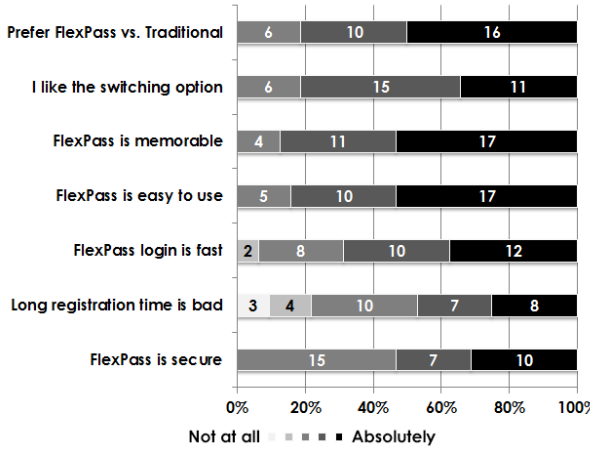

Figure 5: Users' ratings on perceived usability, memorability and likeability.

4 INITIAL EVALUATION RESULTS

We conducted an evaluation study to elicit the users' perceived usability, memorability and likeability towards the proposed method. A total of 32 individuals participated, ranging in age from 20 to 49 (m=33.84; sd=9.43). Participants were asked to rate their experience with FlexPass as well as compare it with their existing, prior experience with traditional passwords in home IoT contexts. Example statements of the survey were: *"I would adopt FlexPass as my main authentication method"*, *"High registration times would prevent me from using FlexPass"*, *"FlexPass login is fast to use"*, etc. Users rated the statements through a 5-point Likert scale (1: Not at all – 5: Absolutely). **Figure 5 and 6** illustrate the users' ratings and comments respectively. Most participants are positive to adopt FlexPass as their main authentication method in their home (81.25%). The same number of participants particularly like the switching option between textual and graphical authentication. 87.5% rated FlexPass as highly memorable. 84.37% find FlexPass easy to use and 68.75% believe that login is fast. When participants were asked to rate the longer registration times required for creating the password key, 46.87% stated that this has not negatively affected their opinion about FlexPass, while 21.87% rated that long registration times might prevent them from using FlexPass. Finally, 53.12% of the participants find that FlexPass is secure, while 46.87% have a neutral opinion.

5 CONCLUSION AND FUTURE WORK

This paper presents a new knowledge-based user authentication paradigm which aims to provide a memorable and adaptable user authentication solution within current highly heterogeneous computational realms in the IoT. Despite, initial encouraging feedback from the performed evaluation study, this approach entails as well new challenges which need to be further explored. Hence, the dual nature of FlexPass embraces new vulnerabilities related to security that need closer attention, *i.e.*, a brute-force algorithm could use the additional information provided by the graphical representation to brake the textual key. Furthermore, the open-ended nature of the suggested paradigm might affect users towards misuse strategies. To assure that users will not create semantically insecure (predictable) grids of images, automated image tagging technologies (*e.g.*, IBM Watson Visual Recognition, Google Vision API, Amazon Rekognition, etc.) and policies need to be investigated to prevent users' unsafe coping strategies. Finally, FlexPass introduces a new kind of observational attack; adversaries know the format of the password (16+ characters) and they can see the set of pictures. Hence, locking mechanisms should be investigated based on a threshold of failed attempts.

Bearing in mind that within nowadays IoT era, end-users authenticate through heterogeneous devices and interaction contexts, it is obvious that current "one-size-fits-all" authentication paradigms might become obsolete. Hence, approaches like FlexPass have the potential to be adopted within diverse IoT-based computational realms. Although initial in-lab experiments are promising, further studies are required to evaluate FlexPass in the wild with the aim to get further insights on its validity, security, user acceptance and real-world user behavior.

"I like the fact that I can choose my preferred way to login. I really feel that the system respects me" ~ P18

"FlexPass was very creative and easy to use." ~ P10

"I had some trouble first. The more time I used it, the easier it became " ~ P22

"It is a more creative way to create passwords" ~ P14

"I really like that I can use pictures as my password" ~ P12

"I had some difficulties in thinking of a secret. Once I defined my secret, the system helped me a lot to build my picture password" ~ P31

Figure 6: Users' comments received at the end of the study.

ACKNOWLEDGMENTS

This research has been partially supported by EU Horizon 2020 Grant 826278 "Securing Medical Data in Smart Patient-Centric Healthcare Systems" (Serums). We thank all participants for their time and valuable comments provided during the studies.

REFERENCES

[1] Antonakakis, M., April, T., et al. (2017). Understanding the mirai botnet. In USENIX SEC 2017, 1093-1110.
[2] Fernandes, E., Rahmati, A., Eykholt, K., & Prakash, A. (2017). Internet of things security research: A rehash of old ideas or new intellectual challenges? IEEE Security and Privacy, 15, 4, 79-84.
[3] Yu, T., Sekar, V., Seshan, S., Agarwal, Y., & Xu, C. (2015). Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things. In ACM Workshop on HotNets 2015, ACM, article 5.
[4] He, W., Golla, M., Padhi, R., Ofek, J., Dürmuth, M., Fernandes, E., & Ur, B. (2018). Rethinking access control and authentication for the home internet of things (IoT). In USENIX Security Symposium 2018, USENIX, 255-272.
[5] Stobert, E., & Biddle, R. Authentication in the home. In Workshop on Home Usable Privacy and Security 2013.
[6] Cranor, L.F. (2014). What's wrong with your pa$$w0rd? TED Talk, March 2014.
[7] Biddle, R., Chiasson, S., & van Oorschot, P. (2012). Graphical passwords: Learning from the first twelve years. ACM Computing Surveys, 44(4), 41.
[8] Wang, J., & Katabi, D. (2013). Dude, where's my card?: RFID positioning that works with multipath and non-line of sight. In ACM SIGCOMM 2013, ACM Press, 51-62.
[9] von Zezschwitz, E., De Luca, A., & Hussmann, H. (2014). Honey, I shrunk the keys: Influences of mobile devices on password composition and authentication performance. In ACM NordiCHI 2014, ACM Press, 461-470.
[10] Findlater, L., Wobbrock, J., & Wigdor, D. (2011). Typing on flat glass: Examining ten-finger expert typing patterns on touch surfaces. In ACM CHI 2011, ACM Press, 2453-2462.
[11] Jermyn, I., Mayer, A., Monrose, F., Reiter, M., & Rubin, A. (1999). The design and analysis of graphical passwords. In USENIX Security Symposium 1999, USENIX Association.
[12] Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A., & Memon, N. (2005). PassPoints: Design and longitudinal evaluation of a graphical password system. International Journal of Human-Computer Studies, 63(1-2), 102-127.
[13] Real User Corporation (2004). The Science Behind Passfaces. Technical report, Real User Corporation.
[14] Mare, S., Baker, M., & Gummeson, J. (2016). A study of authentication in daily life. SOUPS 2016, USENIX, 189-206
[15] Nicholson, J., Coventry, L., & Briggs, P. (2013). Age-related performance issues for PIN and face-based authentication systems. In ACM CHI 2013, ACM Press, 323-332.
[16] Ma, Y., Feng, J., Kumin, L., & Lazar, J. (2013). Investigating user behavior for authentication methods: A comparison between individuals with Down syndrome and neurotypical users. ACM TAC, 4(4), article 15, 27 p.
[17] Katsini, C., Fidas, C., Raptis, G., Belk, M., Samaras, G., & Avouris, N. (2018). Influences of human cognition and visual behavior on password strength during picture password composition. In CHI 2018, ACM, paper 87.
[18] Paivio, A. (2006). Mind and its evolution: A dual coding theoretical approach. Lawrence-Erlbaum, Mahwah, NJ.
[19] Al-Ameen, M.N., Wright, M., Scielzo, S. (2015). Towards making random passwords memorable: Leveraging users' cognitive ability through multiple cues. In ACM CHI 2015, ACM, 2315-2324.
[20] Tulving, E. (2002). Episodic memory: From mind to brain. Annual Review of Psychology, 53, 1-25.
[21] Squire, L (1992). Declarative and nondeclarative memory: Multiple brain systems supporting learning and memory. Journal of Cognitive Neuroscience, 4(3), 232-243.
[22] Williams, H. L., Conway, M. A., & Cohen, G. (2008). Autobiographical memory. In G. Cohen & M. A. Conway (Eds.), Memory in the Real World (3rd ed., pp. 21-90). Hove, UK: Psychology Press.
[23] Baddeley, A. (1990). Human memory: theory and practice. Lawrence-Erlbaum, London.
[24] Stobert, E., & Biddle, R. (2013). Memory retrieval and graphical passwords. In SOUPS 2013, ACM, article 15, 14 p.
[25] Komanduri, S., Shay, R., Kelley, P., Mazurek, M., Bauer, L., Christin, N., Cranor, L., & Egelman, S. (2011). Of passwords and people: Measuring the effect of password-composition policies. In CHI 2011, ACM, 2595-2604.
[26] Burr, W.E., Dodson, D.F., & Polk, W.T. (2006). Electronic authentication guideline. NIST Technical Report.
[27] Atkinson, R.C., & Shiffrin, R.M. (1968). Human memory: a proposed system and its control processes. In: Spence, K.W., Spence, J.T. (eds.) The psychology of learning and motivation (Volume 2). Academic Press, 89-195.