Arias-Cabarcos, P.; Marín, A.; Palacios, D.; Almenárez, P.; Díaz-Sánchez, D. (2016). Comparing Password Management Software: Toward Usable and Secure Enterprise Authentication. *IT Professional*, v. 18, n. 5, pp. 34-40.
DOI: 10.1109/MITP.2016.81

Comparing Password Management Software: Towards New Directions in Usable and Secure Enterprise Authentication

Patricia Arias-Cabarcos[1], Andrés Marín[1], Diego Palacios[2], Florina Almenárez[1], Daniel Díaz-Sánchez[1]
[1]Telematic Engineering Department, University Carlos III of Madrid, Leganés, Madrid (Spain)
[2]Telefónica España, Madrid (Spain)
{ariasp, florina, amarin, dds}@it.uc3m.es, diego@diego.hk

Abstract- In today's corporate IT systems there is an undeniable pattern that is routinely repeated by employees: access to a huge number of password-protected services. In this regard, though deploying a strong enterprise password policy is a mean to increase security against online breaches and data leaks, it also imposes a significant usability burden for users. To alleviate this problem, Password Managers (PMs) are pointed out as user-friendly tools that automate the processes of password generation and login. But how secure and usable are these tools? In this paper we analyze the four most popular PMs with free version from both security and usability perspectives. The comparison leads to recommendations on enterprise PM selection, as well as to the identification of new lines of research and development on usable authentication.

Introduction

Nowadays, we are constantly asked to prove our digital identities: e.g., when performing a check in for a flight, for concluding a purchase via credit card, or in order to log onto a computer or secure web site. This panorama does not change inside corporate walls, where employees need to daily access a huge number of services, whether on-premises, or cloud hosted, or run by partner companies, etc. To face this mental burden of managing an increasing number of accounts and passwords, it is common for users to devise dangerous password strategies, such as reuse or writing down. These bad habits may cause harm to individuals, but the impact is much worse for companies, where a breach on an employee password may leak highly sensitive data and cause important business and reputation damages. These stories have been front page news in recent years [1] and so companies are taking measures, being the implantation of strict password policies the most popular one. Generally, best practices and recommendation guidelines for password policies [2] [3] include restrictions on minimum length and charsets, imposing frequent changes and prohibiting reuse. Despite these mechanisms should imply an increase on security, studies unveil that the stricter the policies, the more are users prone to develop insecure practices in order to cope with the mental burden these policies may impose [4] .

Some new authentication approaches have emerged to provide more security, such as those relying on Single Sign-On (SSO) protocols (see "Related Work" for details), but since passwords continue to dominate the authentication landscape, Password Managers (PMs) are an alternative for immediate adoption without important infrastructure modifications. PMs automate generation of passwords and login processes, which has a direct impact in economic benefits: on the one hand, it reduces the costs of helpdesk calls related to password issues; and on the other hand it minimizes the time employees dedicate to tasks that are not related to their work (login tasks are considered interruptions).

Considering the above mentioned benefits brought by PMs and the recent studies recommending to use these tools [5] , we wanted to evaluate the real security and usability levels of the most popular PMs. The goal of this paper is therefore to perform a comparative analysis, based on expert knowledge and empirical studies with users, and also to derive new directions towards secure and usable authentication schemes for enterprise environments.

Related Work- SSO Protocols and Smart Authentication Clients

The traditional *silo*-based identity scheme, where users are requested to set up *one login per service*, has become inefficient for the current demands of cross-organization cooperation, partnership and collaboration. In order to cope with the identity problems, such as unmanageability and scalability, that arise in current distributed ecosystems there are several technological mechanisms that can be classified into two categories: On the one hand, **SSO protocols** are oriented to provide **credential reuse** functionality, i.e., a user authenticates once and gains access to multiple sites without having to re-authenticate again because information is transmitted between all the involved parties in a seamless manner. Based on this Single Sign-on concept, this last decade witnessed the development of a number of identity protocols built around web services and beyond [1], which include SAML, OpenID Connect and OAuth. The problem with SSO protocols is that the involved parties must create a *Circle of Trust* before authentication data can be shared. Thus, since it is impossible to have a unique federation where all services trust one party for authentication, users end up being part of different federations and so having to actively authenticate many times. The interesting thing would be to combine and complement SSO technologies with mechanisms that enhance password-based authentication.

On the other hand, there are a group of proposals dedicated to alleviate the number of repetitive tasks when managing multiple accounts by moving this load to devices that become **smart authentication clients**. The most salient work on this line is PICO [2] [1] , which envisions users carrying a dedicated authentication device that stores all user cryptographic secrets or credentials and performs automatic logins to web applications and other protected systems on behalf of the user based on a new protocol. But the most promising research lines are those centered on implicit authentication [2] , whose foundations lie on determining user authentication by analyzing behavioral patterns. The main problem of PICO to be adopted in the short term is that it requires important software modifications on services, aiming at totally replacing

password-based authentication. In turn, implicit authentication allows for a better session management by detecting user presence, but neither does it completely eliminate multiple password-based logins. Therefore, the most realistic strategy nowadays is the adoption of Password Managers (PMs), which are software programs that are able to automatically fill password-based login forms and can be used in conjunction with SSO protocols and implicit authentication solutions.

References

[1] Pérez-Méndez, A., Pereniguez-Garcia, F., Marín-López, R., López-Millán, G. and Howlett, J. (2014) "*Identity federations beyond the web: a survey*." IEEE Communications Surveys & Tutorials, Vol.16, no. 4, pp. 2125-2141.

[2] Stajano, F., Jenkinson, G., Payne, J., Spencer, M., Stafford-Fraser, Q. and Warrington, C., (2014). "*Bootstrapping adoption of the pico password replacement system*". In Security Protocols XXII, pp. 172-186.

[3] Hassan, K., Hengartner, U., and Vogel, D. (2015). "*Usability and Security Perceptions of Implicit Authentication: Convenient, Secure, Sometimes Annoying*." Eleventh Symposium On Usable Privacy and Security.

[4] Arias-Cabarcos, P., Almenarez, F., Trapero, R., Diaz-Sanchez, D. and Marin, A., (2015). "*Blended Identity: Pervasive IdM for Continuous Authentication*". IEEE Security & Privacy, (3), pp.32-39.

Comparison of Password Managers

A Password Manager is a software application that aids users in creating, storing, and organizing passwords. Basically, the application creates a local database to save all user passwords, which are encrypted in order to guarantee an adequate protection level. Thus, the user just needs to memorize a single, ideally very strong password, the Master Key, which grants user access to the entire password database. Additionally, many PMs include extra functionalities to improve usability, such as browser plugins to automatically fill login forms on behalf of the user, or synchronization of the password database among multiple user devices based on cloud server storage.

Among all the existing PM software, there are four that outstand because of their popularity: Dashlane, KeePass, 1Password and LastPass. Next, we focus on the analysis and comparison of these four applications.

Usability Analysis

For the **usability study** we consider the set of evaluation criteria known as the 5 E's [4] According to this, usable software must be:

- *Efficient.* Efficiency can be described as the speed (with accuracy) in which users can complete the tasks for which they use the product.
- *Effective:* Effectiveness is the completeness and accuracy with which users achieve specified goals. It is determined by looking at whether the user's goals were met successfully and whether all work is correct.

- *Engaging:* An interface is engaging if it is pleasant and satisfying to use. The visual design is the most obvious element of this characteristic. Equally important is the style of the interaction which might range from a game-like simulation to a simple menu-command system.
- *Easy to learn:* An interface which is easy to learn allows users to build on their knowledge without deliberate effort.
- *Error tolerant:* An error tolerant program is designed to prevent errors caused by the user's interaction, and to help the user in recovering from any errors that do occur.

Based on this set of criteria, the usability of the four PMs was tested empirically through questionnaires with real users. The questionnaires were structured around a set of tasks based on a pioneering study that analyzed two emerging PMs in 2006 [7] . These tasks, which cover the main functionalities of a PM, are described in the list below:

- **Task 1 – Initialization**: register with the PM software and store a couple of personal passwords associated to frequently visited websites.
- **Task 2 – Log in**: start a session in a website for which the PM has a stored password.
- **Task 3 – Remote Log in:** start a session in a website for which the PM has a stored password using a different user device. This task serves to understand portability and synchronization between devices in the user's personal network.
- **Task 4 – Password change:** use the PM to change a personal password for a particular website.
- **Task 5 – Log in with changed password:** complete a log in procedure after a password change.

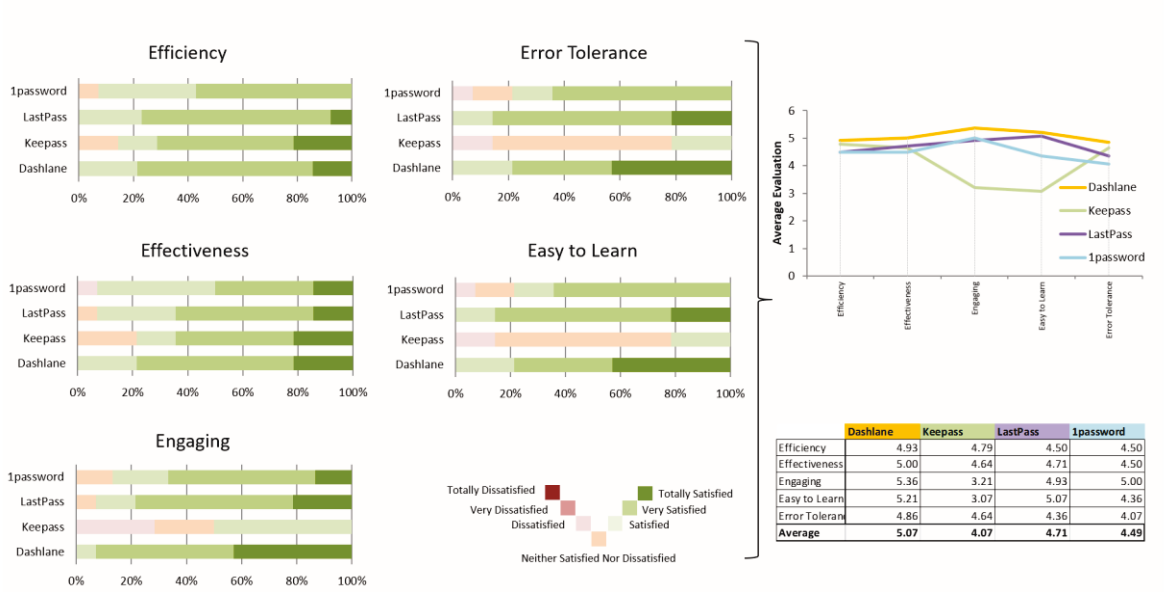
Each respondent followed the set of tasks for each of the 4 PMs under study and gave an evaluation regarding the usability criteria. For rating each criterion, participants were presented with a 7-dimension Likert scale containing labels: "*Totally Satisfied -TS*", "*Very Satisfied -VS*", "*Satisfied -S*", "*Neither Satisfied Nor Dissatisfied - NSND*", "*Dissatisfied -D*", "*Very Dissatisfied - VD*", and "*Totally Dissatisfied -TD*". Furthermore, scale dimensions were assigned a numerical value (decreasing integer from 6 to 0) in order to compute an average quantitative punctuation for each PM.

The usability study involved 14 participants, a number high enough to identify most usability problems as justified in [8] ; and data were collected and processed through online questionnaire tools. All the evaluations are gathered in Figure 1a.

The study reveals that users rate all the PMs with high punctuations in regard to "*Efficiency*", "*Effectiveness*" and "*Error Tolerance*". Rating values are in most cases close to 5 over 6 and no significant variance exists between the evaluations of the different managers. However, important differences between arise when users rate the PMs according to the features of "*Engaging*" and "*Easy to Learn*". For these latter aspects we can see a difference of more than two points between the highest and lowest rated PM, being KeePass the worst evaluated manager in both categories. Furthermore,

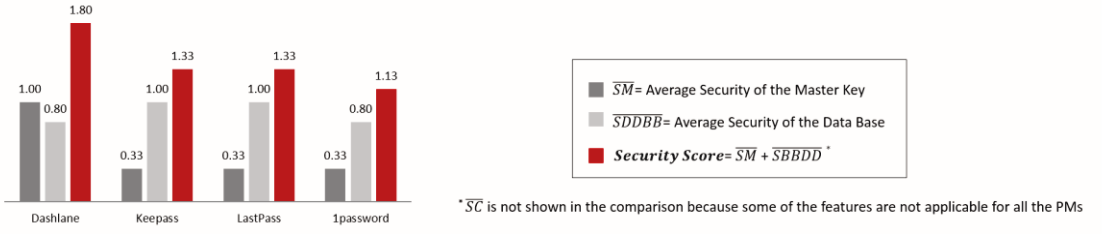
it is to highlight the generally positive nature of the evaluation: no PM gets an average evaluation under 3 points in any of the 5 E's.

From the usability analysis we conclude that users show acceptance of PMs, so moving towards the adoption of this technology is a good choice to enhance passwords-based authentication in the short term, especially in the enterprise arena. Nevertheless, it is crucial that the PM selected by a corporation to be used by employees is engaging and has an easy learning process in order to make the transition smoother. Comparative results are graphically summarized in Figure 1a, where it can be seen that Dashlane outstands over the rest of the analyzed PMs.



	Dashlane	Keepass	LastPass	1password
Efficiency	4.93	4.79	4.50	4.50
Effectiveness	5.00	4.64	4.71	4.50
Engaging	5.36	3.21	4.93	5.00
Easy to Learn	5.21	3.07	5.07	4.36
Error Toleran	4.86	4.64	4.36	4.07
Average	**5.07**	**4.07**	**4.71**	**4.49**

a) Usability comparison



b) Security comparison

Figure 1: Comparative analysis of the usability (a) and security (b) of PMs.

Security Analysis

For the **security study** we decided to use a heuristic evaluation approach and analyze the PMs based on their compliance level to widely-accepted security guidelines, more specifically we build on NIST guidelines covered in [9] and [10] . The set of criteria that guide the evaluation process are based on the general PM architecture, considering the weak points where security must be enforced:

- *Security of the Master Key*. Since the Master Key gives access to all user passwords stored in the PM, it must be strong enough to prevent leaks and attacks. We check: 1) if the PMs impose a mandatory minimum length for the Master Key; 2) if the PMs force the users to create strong Master Keys by applying a secure policy; and 3) if the Master Key is securely stored.
- *Security of the Credentials Database*. This is the valuable asset protected by the PM. We check: 1) the strength of the algorithm used for encrypting the database, 2) if the PMs give quantitative or qualitative feedback on the security level of the stored passwords, 3) if the PMs are able to automatically generate strong passwords on behalf of the users, 4) if multifactor authentication is permitted, and 5) if the PMs allow to schedule password validity periods and generate new password when the configured passwords expire.
- *Security of the Communications*. Security must be guaranteed when communicating credentials between PMs and applications using passwords. We evaluate: 1) the communication security between PMs and external cloud servers; and 2) the communication security between PMs and browser plugins.

Table 1 summarizes the results of the security study, which are also graphically represented in Figure 1b. In order to compare the different PMs, we have assigned quantitative values to each criterion. The majority of the criteria are evaluated using a binary scale so they are given a value equal to 1 if the security feature is supported and 0 otherwise. For those criteria were a security algorithm in use must be specified, we use a continuous scale [0-1] and assign the value depending on the algorithm strength according to well established security recommendations in [9] [10] .

According to the information gathered during the study, the security of the Master Key is protected in all the analyzed PMs in relation to criterion SM#3: the Master Key is never stored, neither locally nor in cloud servers. Instead, a Password-based Key Derivation function is used, which consists of applying a pseudorandom function (hash, cipher, or HMAC) to the Master Key along with a salt value and repeating the process many times in order to obtain a derived key to be used in the rest of PM operations. The added computational work makes password cracking much more difficult, and is known as *key stretching*. However, only Dashlane provides additional security measures for securing the Master Key. This PM forces the user to choose a password with minimum length 8 characters, including an upper case letter, a lower case letter and a number. This policy leads to an increased entropy value of the selected word, and so security against brute force attacks is enhanced.

In regard to the security level of the credentials database all the PMs provide comparable solutions, supporting AES with 256 bits key as cipher, which are the algorithm and key size currently recommended for the highest security. The only difference in this security category lies on the support of automatic scheduling of passwords, only provided by Keepass and LastPass. This feature is important because it facilitates an easy way to limit the validity of passwords, and frequent changes of passwords lead to better security since exposure is shorter in time.

Security Goal	Criterion	DASHLANE	KEEPASS	LASTPASS	1PASSWORD
Security of the Master Key (SM)	**SM#1**. Minimum mandatory length	YES (1)	NO (0)	NO (0)	NO (0)
	SM#2. Forces user to apply policy for strong Master Key	YES (1)	NO (0)	NO (0)	NO (0)
	SM#3. Master Key securely stored	YES (1)	YES (1)	YES (1)	YES (1)
Security of the Credentials Database (SDDBB)	**SBBDD#1**. Algorithm used for DDBB encryption	AES, 256 bits key (1)	AES/Twofish, 256 bits key (1)	AES, 256 bits key (1)	AES 256, bits key (1)
	SBBDD#2. Does the PM give feedback on the security level of the stored passwords?	YES (1)	YES (1)	YES (1)	YES (1)
	SBBDD#3. Automatic generation of strong passwords on behalf of the users	YES (1)	YES (1)	YES (1)	YES (1)
	SBBDD#4. Multifactor authentication	YES (1)	YES (1)	YES (1)	YES[1] (1)
	SBBDD#5. Capability of scheduling password validity periods and generating new passwords upon expiration.	NO (0)	YES (1)	YES (1)	NO (0)
Security of the Communications (SC)	**SC#1**. Security of the communication algorithm between PM and external servers	HTTPS with TLSv1.2, AES 128 and Ephemeral Diffie Hellman (1)	Not Applicable (NA)	HTTPS with TLSv1.2, AES 128 and Ephemeral Diffie Hellman (1)	Not Applicable (NA)
	SC#2. Security of the communication algorithm between PM-browser plugin	AES 256 (1)	Not Applicable (NA)	Not Applicable (NA)	Not Applicable (NA)

Table 1: Security evaluation of PMs. Quantitative value is given inside parentheses for each criteria.

[1] Only for MAC OS and iOS

Finally, the security level of the communications exposes some differences. On the one side, only Dashlane and LastPass provide on-cloud storage. For these two PMs, communication with the storage servers is secured using HTTPS with cryptographic algorithms currently considered as highly secure. More specifically, the protocol version is TLSv1.2 using with AES for confidentiality combined with ephemeral Diffie-Hellman for key exchange between client and server. This kind of ciphersuites provide perfect forward secrecy, ensuring long-term confidentiality of the session, i.e., the compromise of a long-term private key used in deriving a session key subsequent to the derivation does not cause the compromise of the session key. On the other side, while all the PMs support browser plugins, only Dashlane provides public documentation about the security of the communication between plugin and application (based on AES-256).

Figure 1b shows the security comparison and the total quantitative security evaluation given to each PM. It is to note that we have not included the SC dimension in the comparison because some features were not supported by all the applications, or there was missing information. However, since cloud storage and plugins are additional functionalities that are not required to have a fully functional PM, we can look at this comparison as a security evaluation of the core PM functionality. As we can see

in Figure 1b, the best *Security Score* is obtained by Dashlane, with a 1.8 out of 2. Nevertheless, it is important to highlight that all the evaluated PMs demonstrate good general security features, being the lowest security score 1.13 points out of 2.

Conclusions and Future Lines

We have analyzed and compared the most popular PMs with free version regarding usability and security and observed two interesting facts: usability is perceived in a very positive way by users, and all the analyzed PMs demonstrate architectures that are theoretically secure according to current best-practice recommendations. More specifically, Dashlane offers the best combination of security and usability characteristics.

Previous related works, such as [7] , showed a user perception of poorer usability, probably because PM applications were still emerging. Nevertheless, the present study reveals that PMs have reached a level of maturity that is adequate to consider successful mass adoption for both personal and corporate environments. In regard to the latter scenario, there are some future research lines that would boost the adoption of PMs, namely: investigation on how to automatically integrate and enforce company security policies with PMs; combination with SSO technologies highly used inside corporate environments, such as SAML and OAuth; and research on usability improvements by merging implicit authentication with PMs as mechanisms for substituting the Master Key. Finally, as future work we would like to develop automatic testing tools that evaluate the security of PMs empirically in order to complement the theoretical analysis given in this paper and cover specific attack scenarios and vulnerabilities as described in [11] .

Acknowledgements

This work was supported partly by the Spanish Ministry of Science and Innovation under project INRISCO (TEC2014-54335-C4-2-R), and by the State of Madrid (Spain) under contract number S2013/ICE-2715 (e-Madrid).

References

[1] Mirante, D., & Cappos, J. (2013). "*Understanding password database compromises*". Dept. of Computer Science and Engineering Polytechnic Inst. of NYU, Tech. Rep. TR-CSE-2013-02.

[2] Scarfone, K., & Souppaya, M. (2009). "*Guide to enterprise password management (draft), NIST Special Publication*, 800-118".

[3] SANS Institute Report (2014). "*Password Protection Policy*".

[4] Inglesant, P. G., & 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*.

[5] Ion, I., Reeder, R. & Consolvo, S. (2015) "*"... no one can hack my mind": Comparing Expert and Non-Expert Security Practices.*" Eleventh Symposium On Usable Privacy and Security.

[6] Quesenbery, W. (2001). "*What Does Usability Mean: Looking Beyond Ease of Use*". In *Annual Conference-Society for Technical Communication* (Vol. 48, pp. 432-436).

[7] Chiasson, S., van Oorschot, P. C., & Biddle, R. (2006, August). "*A Usability Study and Critique of Two Password Managers*". In Usenix Security (Vol. 6).

[8] Virzi, R.A. (1992). "*Refining the test phase of usability evaluation: How many subjects is enough?*" Human Factors, Vol. 34, pp. 457–468.

[9] Barker, E. (2016). "*Recommendation for Key Management, NIST Special Publication 800-57 Part 1 Rev. 4*."

[10] Polk, T., McKay, K., & Chokhani, S. (2014). "*Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. NIST Special Publication, 800 – 52*".

[11] Li, Z., He, W., Akhawe, D., & Song, D. (2014). "*The emperor´s new password manager: Security analysis of web-based password managers*". In *23rd USENIX Security Symposium (USENIX Security 14)*.

Biographies

Patricia Arias-Cabarcos is a researcher at the University Carlos III of Madrid (UC3M), where she obtained a PhD in Telematics Engineering. Her interests include identity management, trust and reputation models and risk assessment.

Andrés Marín is associate professor at UC3M and holds a PhD in Telecommunication Engineering from UPM. His research interests include ubiquitous computing: limited devices, trust and security in NGN.

Diego Palacios earned a MSc in Cyber Security from UC3M in 2015 and currently works at Telefónica as a Cyber Security Analyst.

Florina Almenárez is associate professor at UC3M, where she obtained a PhD in Telematics Engineering. Her research interests include trust and reputation management models, identity management and security architectures in ubiquitous computing.

Daniel Díaz-Sánchez is associate professor at UC3M, where he obtained a PhD in Telematics Engineering. His research interests include distributed authentication, authorization and content protection.