Poster: Balancing usability and security in the business cloud authentication

Joona Kurikka
Aalto University School of Science
P.O. Box 19210
FI-00076 Aalto, Finland
j@wr.fi

Marko Nieminen
Aalto University School of Science
P.O. Box 19210
FI-00076 Aalto, Finland
marko.nieminen@aalto.fi

1. INTRODUCTION

The increasing amount of cloud services is creating many new ways for remote workers, outsourcing partners - and hackers as well - to access the essential tools and business data of the cloud-enabled companies. As the amount of business critical data in the cloud services increase, so does the need for securing it. Securing a cloud service needs balanced defenses against many different attack vectors in various levels of the service, starting from the edges of the public network and continuing deep inside the individual design of the each software component of the cloud service.

One of the biggest directions for attacks is the route that has to be left open for the legitimate users to use the service – user authentication. The goal for this study was to find balance between making the user authentication in business cloud services secure enough without compromising the usability of authentication. Authentication has to be secure enough to prevent malicious attackers from gaining access to the valuable data and resources inside the service. At the same time it must be usable enough for the legitimate users to be able to access their cloud services efficiently and without unnecessary frustration.

This paper presents the results of master thesis work on balancing usability and security in business cloud authentication. The thesis is available at Aalto University thesis library (aaltodoc.aalto.fi).

2. TEST DESIGN

2.1 System for multi-factor authentication

The performed study was set up to evaluate two-factor authentication: user ID and password-based login combined with three different delivery methods of one-time passwords (OTP): SMS, email and mobile software token ("pledge"). The technical setup was built with the live authentication demo by Nordic Edge, a McAfee- owned company that specializes in secure authentication products. The setup was built around three Nordic Edge products, One Time Password Server, Password Self Service and Mobile Software Token Pledge.

2.2 Subjects of the study: Demographics

Six people (N=6) were interviewed for the study. Half of them were male and half were female. The average age of participants was 25 years and they all reported having two or three years of work experience. They were either finalizing their master degree or graduated during the past year. The educational backgrounds of the participants were as follows: Information and Service Management, Structural Engineering, Industrial Design, Information Networks, UX & Concept Designer, and Product Development.

Due to the small amount of participants in the study, the group was rather homogeneous considering some of the demographic criteria. We consider the study to illustrate how young professionals with academic education would consider such types of authentication. However, as the business cloud authentication solutions are usually implemented for the whole company, the results might not be directly applicable for all business environments.

2.3 Methods and tasks

The evaluation of usability for the authentication tasks is based on the standard definition of usability by ISO 9241-11 [1]. It defines usability through three parameters: effectiveness, efficiency and satisfaction.

The participants were asked to do a complete a login to a remote desktop ("Desktop as a Service", "Desktop Cloud") that would enable them to use all intranet services provided by their company. The login initiated from the public Internet.

Effectiveness was measured in terms of task completion, amount and seriousness of task-hindering issues and amount of help requests for the supervisor.

Efficiency was measured with the task completion time of the whole login process for each authentication method. The measuring of the time begun when the user started typing his email address and ended after the first landing page (the desktop) was visible after a successful login.

Satisfaction was measured with attitude questionnaires after each authentication method. The attitude questionnaire was adapted from previous studies [2, 3], consisting of 18 statements about usability-affecting factors [4], each measured with a 7-point Likert scale. The questionnaire included an equal number of positive and negative statements in random order to create a counterbalancing effect, as it is easier for a human mind to agree than disagree with question statements [5]. The users were also asked to rank each method, overall, on a 30 cm scale from best to worst. The same scale was also used for two other factors of the methods: perceived security and convenience of the methods.

3. RESULTS

Satisfaction was measured with a seven-step Likert questionnaire. The users were presented with 18 statements after testing each of the three authentication methods. The average scores for each statement were calculated and the mean usability scores for each tested authentication method (Table 1) were further derived from these answers.

SMS was evaluated with positive attitudes (over 5 (out of 7) on the Likert scale) on 44,4% of the attributes. The lowest result

came from the need for improvement, but this attribute was consistently low on each of the tested methods, as all of the participants had some ideas for improving the methods. On the positive side, SMS was praised for its simplicity and speed of use.

Email got the smallest amount of positive attitudes (38,9%). It also had three borderline-negative attributes: lack of trust, most need for improvement, and least likable for using the method again. However, email was experienced as a convenient and easy to use solution that did not require any instructions.

Pledge (mobile software token) got the most positive attitudes (50%) and it had only one attitude that was significantly worse compared to the other methods: knowing what to do next. On the positive side, Pledge excelled on degree on trust, reliability and getting the highest score in the question whether the participants would use the method again. One participant commented that Pledge even felt more familiar way to authenticate than SMS and email, even though she reported having no previous experience with any strong authentication methods: "This might be a bit old-fashioned way of thinking, but pledge feels almost like a paper version, like the PIN code lists that you get from the bank".

Overall, however, the methods performed equally well in the evaluation. There were no clear peak attributes inside any of the methods. The overall score between the methods was also quite even, as the difference between the best and the worst mean usability rating was only 0.35 on a scale of 7 (Table 1).

Table 1. Mean results on usability

	SMS	Email	Pledge
Mean	4,91	4,56	4,75
Standard Deviation	2,67	3,04	2,79
N	6	6	6

The participants rated their overall preference (quality) of the three compared methods on a 30 cm scale. They also evaluated separately the security and convenience of the methods on the same scale. As the users were encouraged to change the rating after testing each method if they felt it was necessary, the ranking score represents their opinion of the ranking of these factors. The mean ratings are shown in Table 2.

Table 2. Overall preference (max value = 30)

	SMS	Email	Pledge
Convenience	19,58	17,58	18,25
Security	18	12,92	20,75
Quality (overall)	20,75	15,83	21,75

In the overall comparison the Pledge was considered best with a difference of 1,0 to SMS. Email was the least preferred solution, losing to Pledge with almost 6 points. From the individual factors, email lost to both SMS and Pledge by almost 5 and 8 points, while the difference between SMS and winning Pledge was 2,75 points. The third evaluation factor, convenience, saw the most even distribution of the three; all the methods were inside a 2-point distribution. Convenience was also the only factor that Pledge lost to SMS, with 1,25 points difference.

For visualization and analysis purposes, the individual attribute scores were scaled so that the top score of one represents the maximum value for each category. The results are presented in Figure 1.

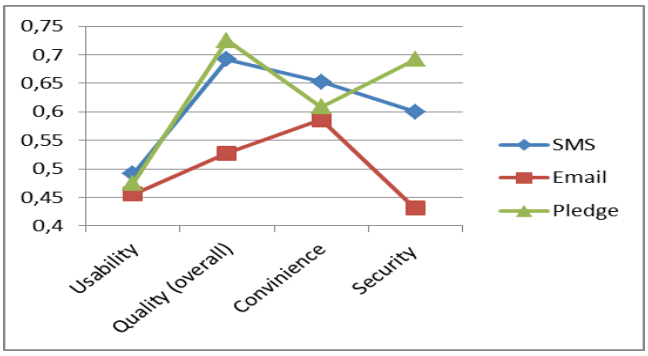

Figure 1. Usability, quality, convenience and security of the methods scores, maximum scores scaled to one.

4. CONCLUSIONS

The overall usability scores of the three studied methods were really close to each other; the difference of the best and the worst method was only 0.35 points on a 7-point scale (5%). The security aspect of the methods had bigger variance in the test scores (26,1%) and the results correlated strongly with the user preference and evaluated overall method quality.

Many of the test participants commented, that if the authentication is done daily or several times a day, as it was described in the test setup, even email OTP would be easy to learn after a few tries and repeat indefinitely after that. One of the test participants commented that "Pledge needs more effort but still feels more convenient than the other methods. The few extra clicks are really easy to learn and repeat with muscle memory without any thinking after that."

Most of the test participants preferred security over usability in the scope of the three tested methods. When given a possibility to select from multiple authentication alternatives, the study participants put more emphasis on the security than usability or convenience. However, during the debriefing interview some of the participants also mentioned that it is important that the usability has to be over a certain threshold, otherwise the security starts to lose importance. Therefore, the *usability threshold of authentication* sounds like an interesting topic to study further.

5. REFERENCES

[1] ISO, 1998. 9241-11. Ergonomic requirements for office work with visual display terminals (VDTs). The international organization for standardization.

[2] WEIR, C., MCKAY, I. and JACK, M., 2007. Functionality and usability in design for eStatements in eBanking services. Interacting with Computers, 19(2), pp. 241-256.

[3] WEIR, C.S., DOUGLAS, G., CARRUTHERS, M. and JACK, M., 2009. User perceptions of security, convenience and usability for ebanking authentication tokens. Computers & Security, 28(1), pp. 47-62.

[4] SHNEIDERMAN, B. and PLAISANT, C., 2004. Designing the user interface, strategies for effective human-computer interaction (international edition).

[5] COLMAN, A.M., 2006. Oxford reference online: A dictionary of psychology. Oxford University Press.