Two Factor Authentication Made Easy

Alex Q. Chen[1] and Weihan Goh[2]
:: Authors' Copy ::

[1] School of Computer Engineering, Nanyang Technological University, Singapore
alexqchen@acm.org
[2] Singapore Institute of Technology, Singapore
Weihan.Goh@SingaporeTech.edu.sg

Abstract. Authentication on the Web is a challenge that can have a negative effect on user experience if it becomes overly complicated and cumbersome. This experience is even more crucial for older and visually impaired users due to their functional abilities. Web applications typically authenticate users by requesting for information that only the user knows (e.g. password). To enhance security, two-factor authentication (2FA) are increasingly implemented, which require the user to manually transfer information between 2FA devices and the Web application. This process can impose usability barriers and stress on human's memory. This paper proposes a technique to mitigate such issues by using wearables as the 2FA device, and to allow authentication information to be transferred seamlessly and automatically from the device to the Web application. From our preliminary results, older users found our approach less stressful on the human's memory and easier to use.

1 Introduction

The presence of adversaries with capabilities to coerce users into surrendering their unique proofs of knowledge (e.g. passwords) strengthens the need for a two-factor authentication (2FA) model. However, providing 2FA on the Web imposes barriers to accessibility and usability. The 2FA model requires users to possess memory abilities and the capability to work between devices or applications to transfer the 2FA information. These requirements impose barriers for visual and motor impaired users; especially for the elderly due to deteriorating memory [18] and cognitive functioning capabilities. These issues suggest a gap to improve the implementation of 2FA in Web applications.

These days, older people are under higher social pressure from family members, such as their children and grandchildren, to use mobile devices [15]. A study on issues faced by old people when using mobile phones suggested that older people use technology only when no alternative method of communication is available [13]. More can be done to help these people adapt to technological advancements, especially when coping with important tasks like security. This paper proposes an approach that incorporates wearables to handle the second factor authentication in Web applications. Our approach is designed to reduce

interaction between devices and users, improving the usability but maintaining soundness and integrity of the security aspects. Our aim is to improve the usability of the 2FA model rather than reinventing it.

2 Accessing Secure Websites

Analysing online security techniques from the usability perspective exposes weaknesses of the system from the human factors element. Often, security processes use widgets as components to construct the user interface of a Web application. Web widgets are components of a Web page that affect how the content is presented and which content to present. Frequently, users are left unaware that changes in the content have taken place [7]. These findings make elderly users vulnerable, as they feel confused when dynamic content is orchestrated without the user's awareness. Highlighting the importance of keeping elderly users aware of the changes to content. Furthermore, introducing new functions to older adults can be intimidating [23]. Older adults are often not confident when using mobile phones. When met with problems, they prefer to recognise and solve them.

Elderly people are less receptive to technology and computer applications than those of younger age. Computer anxiety, fluid intelligence, and crystallised intelligence are important predictors of acceptance for older adults [9]. One of the main factors includes memory performance directly affected by social context [8]. The feeling of being stereotyped by ageing and memory has direct influence on the relationship between age and memory performance.

Service providers are adopting 2FA solutions because it can improve security at lower user effort [21], and improvements to existing security challenges, such as reinventing CAPTCHA to make it accessible to visually impaired users [12] has also been attempted. However, [12] only attempts to make CAPTCHA more accessible rather than improving the model so that it will integrate with existing systems and reduce the overall barriers imposed by the CAPTCHA model. Others attempted to address the accessibility barriers from another perspective. One study designed a generic tool to assist older users when interacting with dynamic Web content [14]. This technique provides help to the user when using a Web page, but it is not capable to deal with dynamic contents that span across multiple devices like what is required of the 2FA model.

Few studies have investigated alternative approaches to implement existing 2FA models on Web applications for the elderly, and the visually and motor impaired. A study covering mobile application trends for the ageing society reported that, commonly, only products and services to provide telemonitoring and alarm systems, user location, and tracking devices are developed [19]. More need to be done to make online security systems and models more intuitive for the ageing and disabled community.

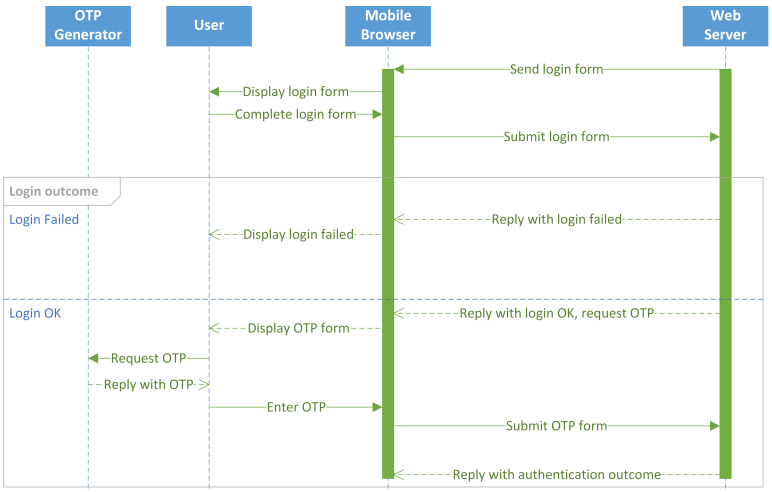


Fig. 1: A high-level overview of a Web 2FA sequence.

3 Authentication Models

Authentication information can be classified as either (1) what the user knows, (2) what the user possesses, or (3) what the user inherently is [22]. The first is ubiquitous - information like passwords falls into such category, and its effectiveness relies upon the non-disclosure of the proof of knowledge. However, with the advent of highly sophisticated coercion techniques and data breaches resulting in the leakage of such information [2, 4], plus bad user practices (e.g. selecting weak passwords [1]), this is no longer the case.

Web service providers (e.g. Google, Dropbox, etc.) have increasingly adopted two-factor authentication (2FA) to mitigate weaknesses in the single-factor authentication model. This typically comes in the form of requesting for a one-time password (OTP) - a single-use code obtainable from the user's OTP device, upon successful completion of the first factor authentication. After receiving a correct OTP, the verifier is entitled to believe that the user has possession of the device capable of generating or receiving the OTP. While there can be many ways to generate OTPs [20, 5], there are Informational and Internet Standard RFCs published detailing standard OTP algorithms [16, 17].

Figure 1 gives a high-level overview of a generic Web 2FA authentication sequence. The difference between 2FA and single-factor authentication can be seen here. The first few transactions up to the submission of credentials via the login form remain the same for both. However, for 2FA, depending on the outcome of the first factor authentication, the Web application would either return a login failure, or request for an OTP. For the latter, the user would submit an OTP obtained from the OTP generator to the Web application.

One of the most common forms of an OTP generator is an OTP token device (see Figure 2a). Such device would require the user to generate an OTP, then

input the digits displayed on the device's screen into the OTP Web form. Another option is to use SMS-based OTPs, where the OTP is generated by a third-party, and sent to the user's mobile device via SMS upon an OTP request. The user would then input the code displayed on the SMS into the OTP Web form.

Additionally, techniques have been developed to simplify the second factor authentication. The Microsoft Account mobile application [3] allows a user to trigger a 2FA authorisation via a button on the application's interface, which then sends the authorisation back to the server via an out-of-band channel. Another 2FA solution, [11], proposes automation of 2FA by geo-location. There is hence a gap in terms of automating the 2FA process to reduce the amount of interaction, and not tie it to specific, external criterion (e.g. geo-location, out-of-band interaction). Part of this gap was mentioned in [6], where the authors discussed the possibility of a smart device communicating an OTP to the browser. Though the authors claimed to have developed a browser extension to that effect and that usability tests were in the positive, however no further reports were provided to support their claims.

We envision that wearables could be utilised to automate the 2FA process. In such an instance, a wearable becomes an OTP generator, producing and returning an OTP when requested by a securely paired device. From there, the OTP is passed to the verifier over the network. This concept can be extended to mobile Web applications, and the entire process can thus be automated, without being tied to external criterion, but instead to the proximity and secure pairing between the wearable and mobile device accessing the Web application.

4 User Evaluation Setup

To better understand existing 2FA implementations and our proposed approach, a collection of phantom applications was developed to simulate how standard 2FA are implemented, and how our approach is perceived. We investigated how participants performed when accessing sensitive data on the Web using a smart mobile phone. The evaluation consists of three investigations: (1) the OTP is sent via a SMS; (2) the OTP is generated by a token device; and (3) using our approach to automate the 2FA process via a wearable device (smart watch). Seven Southeast Asian Chinese participants were recruited: 3 within the University and 4 from the neighbourhood residents' committees. Their age ranged between 51 and 72 years old, with a mean age of 59, of which 4 are males and 3 females. All participants are right-handed and have never used a smart watch prior to the investigations. All participants have experience with smart phones and proof of knowledge authentication (e.g. passwords), but only six have used proof of possession authentication (second factor authentication).

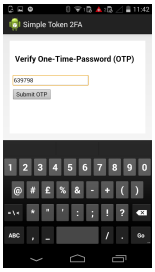
Three sets of phantom applications were developed to simulate the generation and processing of 2FA information. Each set of applications consists of two parts - an Android mobile Web browser application implementing a WebView instance, and a phantom Web application residing on a server within the University. The phantom mobile browser provides an interface between its code and the Web

(a) OTP token device.

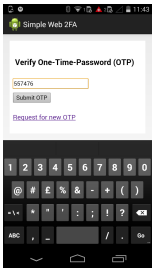
(b) Wearable OTP device.

Fig. 2: OTP generators.

(a) Initial login screen.



(b) OTP form (Token 2FA).



(c) OTP form (SMS 2FA).

(d) Alert simulating SMS OTP.

Fig. 3: Web application components for the Token and SMS investigations.

application, accessible via JavaScript, and statistics such as number of clicks and elapsed time for the evaluation were gathered. The phantom browser for the SMS investigation is capable of generating alerts simulating SMS OTP messages (see Figure 3d) and synchronising of the OTP with the phantom Web application. The phantom applications for the Token investigation, on the other hand, do not verify the OTP submitted, though participants were not told of this and are asked to key in the digits exactly as shown on the OTP token (token used is shown in Figure 2a). For the Watch investigation, a listener was implemented on the wearable to trigger a short vibration and display a notification (see Figure 2b) once an OTP request message is received from the phantom browser. The entire second factor authentication does not require participants to transfer the OTP.

In all investigations, phantom mobile Web applications simulate a 2FA-capable online banking site. Each of them has similar login screens (see Figure 3a) to request for a user identification and PIN. Once the entire authentication process is completed successfully, the participant is shown a menu screen displaying common online banking transactions. Their difference, however, is in the second factor authentication - for the Token and SMS investigations, participants are required to enter the OTP as shown on the token and simulated SMS respectively into the OTP forms (see Figures 3b and 3c), while for the Watch investigation, no user intervention is required for the second factor authentication.

User Studies

Investigation (1) requires the participant to interact with a smart mobile phone when using mainstream 2FA processes, while investigation (3) uses a smart mobile phone and a smart watch to evaluate our suggested approach. Investigation (2) uses a smart mobile phone and an OTP token commonly issued by banks in Singapore. An Android smart phone (Motorola Moto G 2nd Generation) and smart watch (LG G Watch) were chosen in our evaluation setup due to their availability and compatibility. The smart phone has a 5-inch 720x1280 touch screen, and the smart watch a 1.65-inch touch screen. All evaluations assume that the smart phone and smart watch were set up and paired for the tests.

The user studies were conducted in random order. Each investigation is repeated 3 times and the mean result is used to get a naturalised set of measurements. To reduce fatigue, participants were asked to do different tasks of the same nature instead of repeating the same task for 3 times. A two-minute training phase was done for all investigations before the actual evaluation was conducted to ensure that participants are familiar with the authentication models. The following set of initial and post evaluation questions were also asked to understand the investigations better from the participants' perspective.

Initial Evaluation Questions

A1 ***What is your experience using a smartphone?*** Five options were provided: More than 3 times a day; at least once a day; a few times a week; rarely; no experience.

A2 ***What is your experience using a smart watch?*** Similarly, 5 options were provided: More than 3 times a day; at least once a day; a few times a week; rarely; no experience.

A3 ***Have you used the 2FA model before? If yes, discuss your experience with the 2FA model?***

Post-Evaluation Questions

C1 ***Of the 3 investigations conducted, which investigation do you prefer? Explain the reasons for your selection.***

C2 ***Using a 7-point Likert scale, rate how confident are you with the method used by the investigations. From the perspective whether the method is secure and sound.*** The participant will rate the 3 investigations individually; 1 is the worst and 7 very secure and sound.

C3 ***Of the 3 investigations conducted, you specified that investigation X method is the technique you feel most confident with. Explain the reasons for your selection.***

C4 ***Using a 7-point Likert scale, rate the ease of use for the 3 investigations.*** The participant will rate the 3 investigations individually; 1 is difficult to use and 7 very easy to use.

C5 ***During the evaluation, did you feel it was memory stressful in any part? If yes, could you name the investigation(s) from the 3 investigations conducted and describe why you felt that way.***

C6 ***Using a 7-point Likert scale, rate the level of stressfulness on your memory for the 3 investigations.*** The participant will rate the 3 investigations individually; 1 not stressful at all and 7 very stressful on the human's memory.

C7 ***Do you have any remarks or suggestions for the pilot study?***

5 Preliminary Results

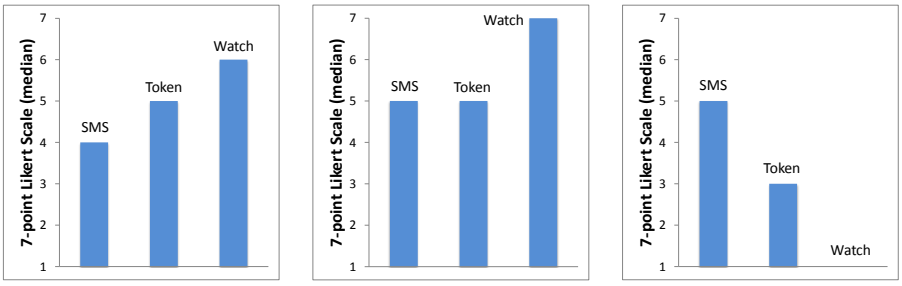
This paper unveils our first steps to overcome the barriers in 2FA-enabled Web applications. In the evaluation, we examined two existing approaches for 2FA in Web applications, against our approach to address the 2FA-imposed barriers users faced. An improvement to accept 2FA when using our approach was noticed. During the evaluation, the performance and usability of all three investigations' approaches were measured. In Table 1, the median time taken to complete the authentication process for the three investigations show that our technique is the quickest. On seven occasions, users took > 1 attempts to pass through the first factor authentication, though most first factor challenge was successfully completed in one attempt. Table 1 also shows the median number of attempts to login and OTP generation for each investigation.

Older participants were noticed to tap more than once to select the textfields while entering their user identification and PIN. This behaviour is especially so when the participant attempts to switch between the user identification textfield and the PIN textfield. Often, most participants seem uncertain what to do with the OTP provided during their first attempt in each investigations (this observation is only noticed for the SMS and Token investigation).

In the post-evaluation questions, 5 participants chose the Watch investigation as their preferred choice (see Table 1) because the approach is simple and automatic. They commented that if the security aspects are dealt with properly, they would prefer to use it. Such responses were surprising, as none of them had used a smart watch before. Two participants mentioned that they do not know

Table 1: Evaluation's measurements and participants choices

	SMS	**Token**	**Watch**
Evaluation Measurements			
Median time taken (seconds)	17.05	16.08	0.27
Median number of login attempts	1	1	1
Median number of OTP generated	1	1	1
Post-Evaluation Questions			
Preferred investigation (C1)	2	0	5
Confidence levels σ	1.13	1.53	1.83
Ease of Use levels σ	2.06	1.63	0.53
Stress on human's memory levels σ	2.23	1.99	0.76
Most stressful on human's memory (C5)	1	6	0



(a) Confidence level. The larger the value the more confident with the approach.

(b) Ease of use. The larger the value the easier the approach was to use.

(c) Stress on human memory. The smaller the value the less stress on human memory.

Fig. 4: Post evaluation questions.

how the smart watch works. They were concerned about the process and security aspects, and they also raised concerns about the smart watch being hacked. The participants were asked in question C5 to choose which investigation that they feel was the most stressful on the human's memory. Six participants chose the SMS investigation, while one chose the Token investigation. The outlier participant (72 years old) was also the only participant that has never used 2FA prior to the evaluation. He raised issues with the small font size on the token's display and the contrast that makes it difficult to read. He also commented that the time provided to read the OTP is too short, thus, he has to request for a new OTP 3 times. The participants were asked to rate the three investigations based on their confidence of the technique (Post-evaluation question C2), the ease of using the technique (Post-evaluation question C4), and how stressful were the techniques on the human's memory (Post-evaluation question C6). The ratings were collected using a 7-point Likert scale and their median results are present in Figure 4 with the standard deviation listed in Table 1.

Users are more confident with the Watch approach than the token and SMS approaches (see Figure 4a). They also found it easier to use the Watch technique (see Figure 4b). Among the investigations, Figure 4c shows that the Watch technique was the least stressful on the human's memory. However, three participants commented that due to the lack of understanding of the security aspects of the Watch technique, they would fall back on the Token approach.

6 Discussion & Future Works

Participants were noted to be wary over the security aspects of the Watch approach, but strongly supported the concepts since it makes the process simpler and quicker, while maintaining the additional security. Further investigation discovered 4 participants describing the Token to be more trustworthy because the banks issued them. Interestingly, none of the participants realised that for the

Token investigation, the phantom Web application could not verify whether an OTP submitted is the same as the one generated by the token. This finding suggests that these participants placed their trust in authority over the technique applied, thus emphasising the need for a new approach, such as ours, to minimise the false sense of security. Finally, at least 3 participants raised their concerns that carrying around security tokens is troublesome and without it one cannot complete the authentication process. These concerns fall in line with the findings reported in [10], which strengthens our case for an alternative approach.

The investigations focus primarily on usability aspects of the Web applications using the three 2FA approaches. As such, security was not implemented in the applications and neither was the complete implementation of the 2FA techniques. Issues with equipment set up and connectivity are also not taken into account. Limitations by the devices and operating systems are also not considered. The small sample size of 7 participants only highlights the main issues of our proposed approach. However, this pilot study is meant only to be a feasibility investigation.

More can be done to improve our approach and minimise the barriers older people faced when challenged with security issues. A more thorough evaluation over a larger pool of participants is suggested for future work. User issues pertaining to Byzantine failures between the devices' communication are also encouraged to be examined. In addition to that, stronger 2FA authentication protocols can be investigated for use in conjunction with our proposed second factor authentication approach.

7 Conclusion

Our investigation revealed that users found existing 2FA-enabled Web applications are not without flaws. Older adults found 2FA tokens can be difficult to read and use, while the SMS technique is stressful on the human's memory. To overcome the usability barriers imposed by the 2FA model, we proposed an alternative approach to automate the 2FA process through the use of wearables, to remove the need for users to be the information conveyor. This reduction in user interaction to complete the 2FA process has proven to be less stressful on the human's memory and makes the experience easier.

Besides benefiting older adults, this pilot study could also assist visually and motor impaired users to adapt to security imposed on mobile devices. We envision that our approach can provide an alternative for second factor authentication; targeting older adults and those less functionally capable, to make 2FA-enabled Web applications more seamless by a broader group of users.

References

1. 2014 business password analysis – trustwave. `https://gsr.trustwave.com/topics/business-password-analysis/2014-business-password-analysis/`, accessed: 2015-02-13

2. Is leaked? https://isleaked.com/, accessed: 2015-02-13
3. Microsoft account - android apps on google play. https://play.google.com/store/apps/details?id=com.microsoft.msa.authenticator&hl=en, accessed: 2015-02-13
4. Security alerts from knowem: Gmail hack. https://securityalert.knowem.com/, accessed: 2015-02-13
5. Alghathbar, K., Mahmoud, H.: Noisy password scheme: A new one time password system. In: Electrical and Computer Engineering, 2009. CCECE '09. Canadian Conference on. pp. 841–846 (2009)
6. Ben-David, A., Berkman, O., Matias, Y., Patel, S., Paya, C., Yung, M.: Contextual otp: Mitigating emerging man-in-the-middle attacks with wireless hardware tokens. In: Bao, F., Samarati, P., Zhou, J. (eds.) Applied Cryptography and Network Security. Lecture Notes in Computer Science, vol. 7341, pp. 30–47. Springer Berlin Heidelberg (2012)
7. Brown, A., Jay, C., Chen, A.Q., Harper, S.: The Uptake of Web 2.0 Technologies, and Its Impact On Visually Disabled Users. Universal Access in the Information Society 11, 185–199 (2012)
8. Chasteen, A.L., Bhattacharyya, S., Horhota, M., Tam, R., Hasher, L.: How feelings of stereotype threat influence older adults' memory performance. Experimental Aging Research 31(3), 235–260 (2005)
9. Czaja, S.J., Charness, N., Fisk, A.D., Hertzog, C., Nair, S.N., Rogers, W.A., Sharit, J.: Factors predicting the use of technology: Findings from the center for research and education on aging and technology enhancement (create). Psychology and Aging 21(2), 333–352 (2006)
10. De Cristofaro, E., Du, H., Freudiger, J., Norcie, G.: A comparative usability study of Two-Factor authentication (2014), http://arxiv.org/abs/1309.5344
11. Grim, E.: Two-factor authentication systems and methods (2013), https://www.google.com/patents/US8578454, US Patent 8,578,454
12. Holman, J., Lazar, J., Feng, J.H., D'Arcy, J.: Developing usable CAPTCHAs for blind users. In: Proceedings of the 9th International ACM SIGACCESS Conference on Computers and Accessibility. pp. 245–246. ASSETS '07, ACM (2007)
13. Kurniawan, S.: Older people and mobile phones: A multi-method investigation. International Journal of Human-Computer Studies 66(12), 889–901 (2008)
14. Lunn, D., Harper, S.: Providing assistance to older users of dynamic web content. Computers in Human Behavior 27(6), 2098–2107 (2011)
15. Mallenius, S., Rossi, M., Tuunainen, V.K.: Factors affecting the adoption and use of mobile devices and services by elderly people–results from a pilot study. Paper presented at the 6th Annual Global Mobility Roundtable, Los Angeles, CA (2007)
16. M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., Ranen, O.: RFC 4226–HOTP: An HMAC-Based One-Time Password Algorithm (2005)
17. M'Raihi, D., Machani, S., Pei, M., Rydell, J.: RFC 6238–TOTP: Time-Based One-Time Password Algorithm (2011)
18. Perlmutter, M., Mitchell, D.B.: The Appearance and Disappearance of Age Differences in Adult Memory, vol. 8, chap. 7, pp. 127–144. Springer US (1982)
19. Plaza, I., Martín, L., Martin, S., Medrano, C.: Mobile applications in an aging society: Status and trends. Journal of Systems and Software 84(11), 1977–1988 (2011)
20. Rubin, A.D.: Independent one-time passwords. In: Proceedings of the 5th Conference on USENIX UNIX Security Symposium - Volume 5. pp. 15–15. SSYM'95, USENIX Association (1995)

21. Sasse, M.A., Palmer, C.C.: Protecting you. Security & Privacy, IEEE 12(1), 11–13 (2014)
22. Shirey, R.: Rfc 4949–internet security glossary (2007)
23. Zhou, J., Rau, P.L., Salvendy, G.: Age-Related Difference In The Use Of Mobile Phones. Universal Access in the Information Society 13(4), 401–413 (2014)