Assessing Usable Security of Multifactor Authentication

Maha M. Althobaiti, Pam Mayhew
School of Computing Science University of East Anglia
Norwich, England

Abstract

Authentication mechanisms are considered the typical method to secure financial websites. Context authentication has become increasingly important in the arena of online banking, which involves sensitive data that belong to users who trust their banks. Multifactor authentication is the most commonly used method of strengthening the log-in process in e-banking. However, developing a usable, secure authentication approach and method is the most challenging area for researchers in the fields of security and Human-Computer Interaction (HCI). This paper presented our new approach for authenticating users who access online banking by giving them the opportunity to choose their preferred method to log into e-banking. In our complex experiment with 100 online banking customers, we simulate an original online banking platform based on the proposed approach; then, we evaluate the usability and security of three different methods (fingerprint, secure device and card reader). The initial results indicate that the new system model was able to assess the usability and security of different multifactor authentication methods, and it is considered a first attempt towards a usable and secure authentication approach. Moreover, fingerprints are considered the most usable and secure method from users' perspectives.

1. Introduction

Banking websites are considered high risk, and overall security is their primary concern, as they are dealing with customers' personal accounts, transaction histories and card data. Security has also become an important issue in the last several years, because the number of banking users has increased; for example, in the United Kingdom, approximately 25 million people used e-banking in 2012 [1]. Authentication mechanisms are the access keys to financial services, and they work to verify users' identities, so they are highly important. Most often, the level of website security depends on the strength of the site's authentication mechanism. Therefore, most e-banking systems use multifactor authentication to provide strong and secure authentication. It is extremely important to bank owners that user security and the usability of banking systems be ensured. However, maintaining user security can also be problematic, because users tend to prefer authentication methods that are simple and, therefore, less secure. Authentication is one of the research fields that explores the conflict between security and usability [2]. Experts in the fields of Human-Computer Interaction (HCI) and security have addressed this conflict and defined new fields for studies on usability and security ('usable security'). Whitten and Tygar [3] defined *usable security* as the user's ability to identify security tasks by avoiding harmful errors and being confident with the system interface. The Computing Research Association [4] identified Human Computer Interaction Security (HCI-SEC) as one of the "four Grand Challenges in Trustworthy Computing".

Few research works and publications have examined the usability and security of authentication mechanisms empirically [5]. Thus, our work will narrow this gap and describes the current empirical study, which we designed and conducted with several parallel goals.

First: we propose our new authentication approach to e-banking. This approach allows the user to choose the preferred method to authenticate to online bank.

Second: we apply our methodology to evaluate the authentication method and process by integrating usability criteria and security criteria that related to the users' role during the authentication process in online banking.

Third: we assess the usability of three different multifactor authentications (fingerprint, secure device and card reader) based on a real experience with each method by a user so more accurate results can be gained.

2. Related Work

An authentication mechanism is a security service that distinguishes between authorised and unauthorised users. Generally, authentication methods are categorised based on the factor used: knowledge-based authentication uses factors such as a PIN and password, token-based authentication uses cards or secure devices, and biometric authentication uses fingerprints. The use of more than one factor is called *multifactor authentication*; most e-banking systems today use this method to strengthen the verification process. Usability and security are both

essential for any secure system or product, including authentication methods, and they should go hand-in-hand, as usability is concerned with easy access to a system and security is concerned with secure access to a system. Few previous studies have empirically focused on the usability and security of multifactor authentication. For example, Weir et al. [6] compared three different token devices as multifactor authentication methods in an experiment with 50 e-banking customers to compare their security, usability and convenience. These devices were a card-activated token, a push-button token and the chip-and-PIN method. The results of the study showed that users considered card-activated tokens usable and secure, but they found the chip-and-PIN method less usable [6]. Our study aims to find a new, usable and secure approach to authenticate users. In addition, we evaluate the security and usability of three kinds of multifactor authentication methods (secure device, card reader and fingerprint) that differ from those used in Weir et al.'s study [6].

3. Approach

Typical online banking provides the user with one multifactor authentication method approach. Therefore, our approach first aimed to provide the user with more than one authentication method. Fig. 1 shows the proposed approach model, which includes clear steps for the authentication process. Second, we aimed to provide a realistic experience. In the domain of usability studies, the aim is usually to encourage users to behave as they do in the real world so the most accurate results can be obtained. Moreover, dealing with sensitive data and banking websites especially requires more effort to encourage users to interact securely, as if they are dealing with their own information in the real world. To achieve the second goal, we simulated a real online banking system and used the researchers' own information (card and token). We hoped this would encourage users to behave securely.

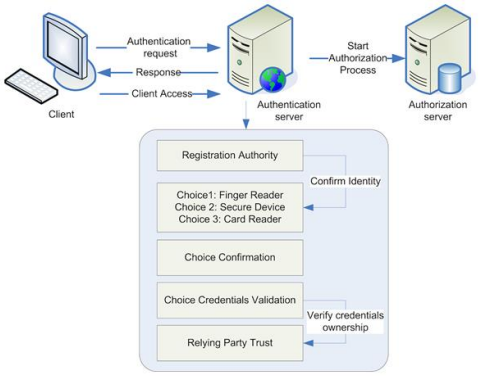

Figure 1. Proposed approach

3.1. Study Questions

The experiment was designed to answer the following questions:

- Is there a new, usable and secure approach to authentication?
- What is the most desirable authentication method employed by online banking users?
- What are the differences between a fingerprint, secure device and card reader in terms of usability, security and trustworthiness from users' perspectives?

3.2. System Design and Study Materials

For the experimental study, a system was programmed to simulate an original online banking system in the United Kingdom (HSBC) following the proposed authentication scenario model in Figure 1. The simulated system provided the user with three kinds of authentication methods (secure device, card reader and fingerprint). HSBC Bank originally used one method, which is a secure device, and the secure device used in this study belongs to the researcher's account with HSBC. The finger reader used in the study is SecuGen Hamster Plus, and the card reader belongs to the researcher's account with Barclays Bank (see Figure 2). The other items used for this experiment include a consent form, an electronic survey, a scenario sheet and an observation sheet.

Figure 2. The used methods

3.3. Study Procedure

- We recruited 100 users in total for our experiment by advertising the experiment in the main library of the University of East Anglia.
- Each user was asked to sign a consent form and was informed that he or she would need to make a payment using the researchers' account and this transaction would be recorded.
- Each user was given a specific ID, and each chose his or her preferred method to log into the website and access the account page (See Figure 3).
- Each user utilised all three different methods: the first method to log into the system, the second to make the payment and the third to confirm personal information to receive a receipt.

- Based on the user's choice, a proper scenario with detailed information about the payment was given to the user to follow.
- At the end of the experiment, the users were asked to complete an online questionnaire to evaluate all the methods involved.
- Finally each user has been thanked and given £5 as a reward for the participation.

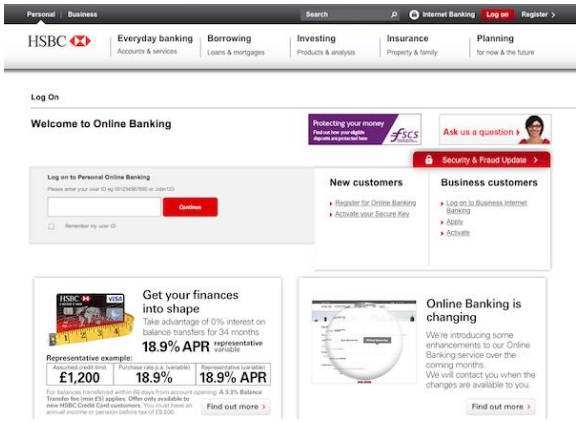

Figure 3. Home page for the simulated system

3.4. Study Scenarios

Regarding the study's requirements, three different scenarios were prepared based on the users' first choice of the first method. For example, if the user's first choice was fingerprint, then he or she was forced to use a secure device to confirm the transaction process and card reader to receive the receipt via an email address. Generally, we had three different scenarios, as can be seen in Table 1.

The reason behind this is that each user who participated in this study would finish with real experience with three different methods. In this case, he or she could fill in the survey and evaluate each method based on recent and real experience with all of the methods. Each scenario consisted of all the details that the user needed to perform the task. The task for this experiment was to log in using an ID, secure question and proposed second method. Then the user followed the requested task to transfer a certain amount of money to a specific person, given all the details for the transfer. By the end, the user needed to confirm the payment and enter a given email address to receive a receipt.

Table 1. Scenarios' design

Scenario 1	Scenario 2	Scenario 3
Fingerprint	Secure device	Card reader
Secure device	Fingerprint	Fingerprint
Card reader	Card reader	Secure device

4. Assessment Methodology

Our assessment approach depended on the necessity of evaluating each method and was due to the unavailability of the existing model to evaluate the authentication process, as most studies applied the normal usability methods. We developed our approach to evaluate the methods by integrating existing evaluation criteria for usability with security criteria that were based on users' awareness of security indicators. These criteria are described below.

4.1. Usability Metrics

In the current experiment, usability was measured through examining efficiency, effectiveness and satisfaction. Efficiency was measured by calculating the time required to use each method. Effectiveness was measured by task completions and numbers of requests for help, either by clicking the help link or asking the observer. Satisfaction was measured through the data collected from the questionnaire, and the factors employed were based on Nielsen's definition of usability [7]. The usability attributes from Nielsen's definitions are: learnability, efficiency, memorability, errors and satisfaction. We have added another two attributes that are required for a secure system: security and trustworthiness.

4.2. Security Metrics

In the current study, security was measured through assessing attention, caution, motivation, wariness and satisfaction. Attention was measured by observing users' awareness and noting a missing 'Secure Socket Layer (SSL)' in the address bar. Caution was measured by observing users' interaction with requested sensitive information, such as entering an email address in an insecure page. Motivation was measured by observing users during their interaction with authentication methods and measuring their progressing with providing a fingerprint and continuing the authentication process. Wariness was measured by observing users' interaction, behaviour and understanding of a warning message during the authentication process. The warning message used in this study dealt with the absence of a security certificate. Satisfaction was assessed through the data collected from the questionnaire after the experiment.

5. Data Collection

Data were collected in three different ways: through our database, as the website created a table scheme to record responses from users to various

options selected or clicked while browsing the webpage. The strategy used for capturing responses was set to FALSE(0) for all expected responses by default and was updated to TRUE(1) when the user selected certain options. The experimenter used an observation sheet as she sat with each participant during the evaluation session to record any difficulties with any of the methods and any comments from participants. The last instrument was the questionnaire, an online survey that included closed-ended and open-ended questions. It was made up of four sections. The first section had ten general information questions. The second section had 10 statements rated on a five-point Likert scale (1=strongly agree to 5=strongly disagree). Each rating was repeated for the three used methods. The third section had four questions to rank the three methods in terms of preference, ease of use, security and trustworthiness. The last section consisted of open-ended questions that asked participants about what they liked and disliked for the used methods.

6. Results and Discussion

In this section, we present our results and preliminary analysis for these results combined with a discussion for each finding regarding the results. We have divided the section to present the demographic data results first, followed by usability and security results.

6.1. Respondents' profile

One hundred users participated in our experiments: 50 female and 50 male (See Table 2 for demographic data). The participants had different nationalities, but the majority of the participants (78%) were British. All the participants belonged to different age groups, levels of education and schools of study. All the subjects had used the Internet for more than three years. Based on this, we can assume that the IT literacy of respondents was high. Regarding the usage of online banking, 3% of our subjects have a banking account but had not used online banking before, while 97% had used online banking before. More specifically, 12 participants had used online banking for less than one year, 54 participants had used it between one to three years, and 31 of them had used it for more than three years. In general, we can consider this a positive finding, as our subjects had previous experience with online banking. We have also investigated whether the subjects have an account with our simulated bank, which is HSBC, and we found that 40% of them have an account with HSBC. Moreover, we investigated whether the subjects have experience in the domain of security. We found that 12% of them have experience in the domain of security, while 88% have no experience in the domain of security. This allows us to compare the results between those who have experience and those who had no experience and observe their interaction more carefully.

Table 2. Demographic data

Gender	
Female	50
Male	50
Age	
18 – 25	65
26 – 30	10
31 – 35	20
Above 35	5
Education	
School	4
College	33
Undergraduate	48
Master's Degree	10
PhD	5
Internet Usage	
More than three years	100
Online Banking Usage	
Less than one year	12
One – three years	54
More than three years	31
Monthly Usage of Online Banking	
0 – 3 times	34
4- 7 times	32
More than 7 times	30
Security Experience	
Yes	12
No	88

6.2. Usability Results

Regarding efficiency, we measured the time spent to learn each method by calculating the time between opening the page and the start time to click on the required button. Fingerprint was the fastest method in terms of learning (mean: 5.7 s) compared to the secure device and card reader. The reason behind this is that fingerprinting does not require several buttons to click or numbers to generate. It has one step: scan a finger on the device. For effectiveness, all participants completed the required task and finalised the requested steps in the scenario. Regarding satisfaction, the researchers have so far conducted a preliminary analysis of the data, which has yielded some very promising results. The data analysed using SPSS software and the users' responses to the ten statements for rating the three methods (fingerprint, secure device and card reader) have been analysed. The results showed that there is a

positive relationship between using a fingerprint and the level of security and usability and Table 3 show the mean values from the Likert scale for each method and it indicates that users feel that the finger method is most usable, the most secure and the most trustworthy. This means that, when the fingerprint was used, the level of usability and security increased. Regarding the last section of questions that asked the users to rank each method in terms of preference, ease of use, security and trustworthiness, the fingerprint was also most preferred by the users.

Table 3. Mean differences between methods

	usability	security	trustworthy
Fingerprint	**3.71**	**4.05**	**3.96**
Secure device	3.08	3.74	3.74
Card reader	3.46	3.78	3.85

6.3. Security Results

As mentioned previously, five criteria assessed the security level of the authentication process regarding the methods by examining the users' awareness and behaviour with the presented security indicators. During the experiment, regarding the observation of users' attention to the missing SSL and availability of a security icon and https in the address bar, none of the 100 users recognised the absence of SSL. However, 12 of the 100 users indicated they had experience in the domain of security, which revealed that the users' attention regarding the understanding the importance of an SSL connection is very low. Caution was measured by observing users' ability to type and provide an email address in an insecure page. During the experiment, all the participants provided and typed an email address in an insecure page without any concern, which also indicates their weak understanding of the harm that could happen as a result. Regarding motivation, which measure users' responses to the request for providing authentication methods, those who used the secure device were happy to use the method and complete the authentication process. Regarding those who used the card reader, 14 hesitated to use the original card. On the other hand, those who used the fingerprint seemed to enjoy the experience, while three out of 100 wondered whether their fingerprint would be saved in the website database, which indicated their caution to provide their fingerprint was not due to working in an insecure page but because of their wariness it would be used in other ways. Finally, wariness was measured by observing users' responses to the warning message that related to the missing security certificate. In this step, we obtained results from the table schema created to record responses and from the observation sheet. The results indicate that 85% of users pressed the OK button, which means they continued the process without any wariness, while 15% pressed cancel to avoid harm or danger. From the observation sheet, the experimenter was able to divide the participants' responses to the warning message into seven groups:

- Those who were confused after reading the message and decided not to go further (1 user).
- The group that read the message very carefully and tried to understand its content (f=16).
- Those who hesitated to proceed with the process (f=7).
- The group (f=5) that requested help from the observer.
- Two that decided to discontinue their work.
- One user who tried to find instructions to help him to decide.
- Finally, 68 users were not concerned and ignored the message.

Generally, the results indicate that the participants' level of attention, caution, wariness and motivation for security during the authentication is weak. In addition, it seems that their background regarding the security of online banking is very low; however, all of them are online banking users.

7. Conclusion

The presented study proposed an approach for evaluating different multifactor authentications by giving users the freedom to choose their preferred method to authenticate themselves while online banking. Our methodology that forces each user to use three different methods was successful and ended with an experiment that gives each user a realistic experience with each method in order to be able to rate each of them and get an accurate result. Moreover, the study's methodology suggested the integration of usability metrics with security metrics that related to the users' awareness of security indicators. The results from the experiment indicate that fingerprinting was the most usable and secure method from the users' point of view. Finally, the users' level of understanding security indicators is very low, based on observing their reaction to the security features presented in the study.

8. References

[1] Hyde, D. (2012). Hackers crack new online banking security putting 25 m people at risk. This is money. Available from: http://www.thisismoney.co.uk/money/saving/article2096060/Hackerscracknew-online. Available online. [Accessed on 13/12/2014].

[2] Nodder, C. (2005). Users and trust: A Microsoft case study. In: L.,Cranor, S.,Garfinkel, editors. Security and Usability. O'Reilly; pp. 589–606 [chapter 29].

[3] Whitten, A., and Tygar, J.D. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In: Proceedings of the 8th USENIX Security Symposium, 99, McGraw-Hill.

[4] Computing Research Association (2003). " Four Grand Challenged In Trustworthy Computing", Final report of CRA Conference on Grand Challenged in Information Security and Assurance, Airlie House, Warrenton, Virginia, November 16 – 19.

[5] Piazzalunga, U., Savaneschi, P., and Coffetti, P. (2005). The usability of security devices. In: L.,Cranor, S.,Garfinkel, editors. Security and Usability. O'Reilly; pp. 221–42 [chapter 12].

[6] Weir, C.S., Douglas, D., Carruthers, M, and Jack, M. (2009). User perceptions of security, convenience and usability for ebanking authentication tokens. Computer & Security, 28(1).

[7] Nielsen, J. (1993). Usability engineering. San Francisco: Morgan Kaufmann.

