06 January 2015

E-banking &Two-Factor Authentication Methods

Literature review- pp.1-9

Author: Cuber, Marcin
SN: 12004964
UNIVERSITY COLLEGE LONDON (UCL)
RESEARCH METHODS- COMP3095

Abstract: This report focuses on Two-Factor Authentication (2FA) methods that can be used for online services such as online banking (e-banking). Online banking classifies to the scenario where everyday users are heavily encouraged to perform critical tasks over the Internet. Currently all high-street banks support online banking because it enables them to serve far more customers than traditional banking, at a very low cost [1]. Websites that require authentication commonly use the static-authentication (i.e. ID/Password) and users accepted it very quickly because it's easy to use. E-banking services advertise 100% security, which is based on security assumptions of the bank. However, this condition is only satisfied when users' fulfil certain security requirements [2]. In consequence users can have a negative impact on security and this risk can be cured by 2FA.

The aim of the literary review is to thoroughly understand the relevant theories relating to 2FA and leads to answering three questions:

Q1. What caused 2FA methods to be outmoded?
Q2. Is there existing method that can potentially be secure and usable in e-banking?
Q3. Can mobile-based authentication proffer e-banking with secure and usable 2FA?

The method chosen to answer these research questions would be experimental research. A range of sources were investigated, critically reviewed and evaluated to establish and identify potential gaps that can be explored in future research.

1 Introduction

E-banking and online communication became our routine task and so old-fashioned customer services were swapped with Internet services. Since services like banks moved to Internet, authentication became essential in order to provide security of privacy. It's argued that trying to increase both security and usability at the same time for the same authentication method is almost unobtainable because if one factor increases the other one drastically decreases [3]. So, the objective of this review concentrates on verifying whether existing methods have the potential of being both secure and usable, and can be adapted in e-banking services.

Existing online services only use one-factor authentication (i.e. ID/password) that provides rudimentary capability to prevent unauthorised access. Security-tokens[1] which generate One-Time-Passwords (OTPs) can be used for the second layer of authentication that could significantly improve the level of security and make it intricate to gain unauthorised access to sensitive data.

Reviewed research papers indicate that implementation of various OTP methods using smartcards, security-tokens or smartphones is effectively ongoing. Security is the key factor that is considered when modern methods are being implemented. Noticeably, use of smartphones to generate OTPs is the area where research is proceeding and expanding.

The motivation to conduct this literature review is driven by a project in which comparative study could potentially be carried-out. Section 2 evaluates 2FA methods, outlines factors for and against 2FA, and also points-out gaps and contradictions in researches. Furthermore, broader evaluations are available which verify factors that influence the adaptation of 2FA.

[1] **security-token**- term refers to dedicated device (hardware) that generates OTPs

2 Literature Review

2.1 Authentication

The most common solution for today's online services is the well-known ID/password approach [4]. It's widely used despite its security gaps which can be exploited by the Internet. The Internet is vulnerable to numerous threats from hackers, unauthorised authorities, cyber criminals, etc. These threats occur in different forms like unprivileged activity, unauthorised access, and manipulation on private data. Nevertheless, static-authentication has many weaknesses as it's considered as a low-security solution when used on its own [5]. To improve security, enforcement password rules are suggested for choosing and maintaining passwords [6]. User should apply following: non-dictionary and no-name passwords, periodic changing, use complex yet easy to remember passwords and passwords shouldn't be shared with other users or be written. Adams and Sasse [1] hypothesised that users are writing their passwords because there is lack of awareness, and their questionnaire validated it with user's quote: "*I don't think that hacking is a problem*". Thinking this way in the 21st century can cause serious problems especially when individuals are making high-value transactions via an e-banking system. Additionally, research [4] indicates that passwords are written because there are too many to remember for different websites.

The major requirement of e-banking is to implement a strong solution for authentication of individuals. Through the process of authentication an individual must prove his/her identity; a credential is then recognised that asserts proof of the individual's identity. There are three authentication components that are available to match an individual to an established credential [7]: possession, knowledge, and inherence. Based on these factors, authentication can be one-factor or multi-factor. Research [7] [8] consistently conclude that usage of one-factor authentication is risky and addition of second factor will provide an extra barrier to fraudulent entry. Comparison of authentication-types is covered in Section 2.4.

2.2 Generality of 2FA

The development of powerful technologies over the 21st century had underlying consequences in hacking technologies becoming more diversified and advanced. Therefore, security offered by one-factor authentication is defenceless to replay-attacks, physical-attacks, guessing-attacks, brute-force-attacks, dictionary-attacks etc. [9] [10]. In order to increase the level of security, services combine multiple authentication factors. The number of authentication factors may be decided based on, transaction types, risk levels, threats and vulnerabilities. However, the main dilemma is to verify and select method that is both secure and usable. Previous publications already conversed on this dilemma in the provision of authentication methods [2] [11] [12]. In addition, empirical studies [7] [13] delineate that the increased security is affecting the usability of the system. The increased security is reflected in the additional layer of difficulty which users' must satisfy in order to log-in. Consequently, this creates the need for instructions that fledgling users have to follow. Furthermore, implementations of 2FA methods shouldn't rely on users' knowledge because usability of the system can be the key to customer's satisfaction and acceptance [14]. Nevertheless, it's argued that users could get locked out of their own accounts by using 2FA; therefore users should also be aware of the risks when adding security [9].

2.3 Complexity and Security

Adapting 2FA methods can bring further complexity to both the understating and the usage of the system. Many bank users prefer carrying out transactions via e-banking making the Internet indispensable, but it also requires some level of technical knowledge and competence. Jeong and Yoon

[15] argue that well-educated people should find e-banking less complex. Also, research [16] concludes that the complexity of 2FA methods has a negative effect on its rate of adoption.

Security is an important factor, which drives the adoption of 2FA in online services. The empirical data in [15] connote that security is the top reason why adaption of 2FA in e-banking is needed. The Internet is part of our daily routines and consequently users are becoming more aware of the safety and security that are needed in the online environment. However, despite increased security offered by 2FA, there are still criticisms, which argue that 2FA will not prevent all the attacks happening in online environment [17]. Moreover, supporters of 2FA counter criticisms with authenticity that users would feel more confident and secure whilst having multiple layers of security. Nevertheless, an extra layer constructs a barrier to users' adoption of 2FA in e-banking because it increases the amount of users' efforts to access their account [3].

2.4 Authentication-Types

Researchers gathered a wide range of possibilities that can improve the security of the system. To compare different methods, three authentication types are devised; knowledge-based, possession-based and biometric-based.

2.4.1 Knowledge-Based

Knowledge-based methods gained largest popularity. These authentications comprehend passwords, pass-phrases, graphical passwords, pass-faces and PINs. It was argued that usability decreases with multiple passwords/phrases that need to be memorised by humans [5] [10]. Consequently, combination of knowledge and possession/biometric should be applied because independently used knowledge-based authentication leads to low security.

2.4.2 Possession-Based

Possession-based methods require users to have a physical object, i.e. smart-card or security-token. These methods are widely used by banks, especially the combination of cards and PINs (2FA) because they're inexpensive and easy-to-use. Security-tokens are more expensive than smartcards because of their complexity and need for dedicated-devices [9]. The complexity behind these devices provides higher security and consequently makes them more difficult to forge.

2.4.3 Biometric-Based

Biometric-based methods concentrate on identifying users' characteristics, i.e. fingerprint, iris, and face. Scanners that are used provide a possibility to recognise characteristics and match them with the individual's identity. Biometric-based methods are highly secure but technically complex and expensive to use because dedicated hardware is required. In addition, methods are perceived to be intrusive; lowering its usability. Biometrics are used in systems that require a high security level [10], but as recognition stage always uses the same template, due to the inalterability, it creates security breach in case template is used by a malicious attacker [18].

2.4.4 Comparison

The factors that are considered when selecting an authentication-type:

F1. Ease of use
F2. User acceptance
F3. Level of Security
F4. Ease of implementation
F5. Cost effective

Knowledge-based methods are inexpensive, easy to implement and also easily form 2FA when are combined with possession-based or biometric-based methods. Additionally, knowledge-based methods are low security because they're easiest to compromise in comparison with generated tokens[2] or biometrics, which are fundamentally more secure. Consequently, token-based and biometric-based authentications are more expensive to implement and users require instructions in order to use them. Users prefer knowledge-based methods and don't look comfortable with biometric-based methods [18].

Table 1 contains a classification of authentication-types according to five factors. Outcome presents similarities found in multiple sources [1] [3] [7] [11] [12] [13] [14] [17] [18].

Table 1. Comparison- Authentication-Types

Authentication-Type:	**F1**	**F2**	**F3**	**F4**	**F5**
Knowledge-based	High	High	Low	High	High
Possession-based	Medium	Medium	Medium	Medium	High/Medium
Biometric-based	Low	Low	High	Low	Low

Table 1 presents stronger and weaker points of authentication-types. This comparison determines that combinations that can form a feasible 2FA for e-banking should use knowledge-based and possession-based methods. Nevertheless, no silver bullet solution exists that can protect users in every single case. Therefore, the following sections evaluate old-school and modern 2FA methods.

2.5 Old-School 2FA Methods, Security-Tokens

The previous section demonstrated and compared three authentication-types. This section contains evaluations of possession-based methods and points-out why some of them aren't used anymore.

The comparative usability studies in [5] [7] [13] compared diverse possession-based methods; most of them carry the old-school nickname because they're hardly used anymore. In general, there are different methods that can generate tokens, i.e. card-activated tokens, push-button tokens, PIN-secured tokens and specific dedicated devices like RSA SecurID or CRYPTOCard (counter synchronised OTP). Above mentioned devices were shelved by organisations because dedicated devices are expensive and users don't accept carrying additional devices. Moreover, technological evolution defeated these methods and substituted modern versions that are more secure and usable. Also, in 2011 information of RSA's SecurID-token were exposed to a malicious attacker by hacking. At the time SecurID were used as part of 2FA for e-banking and this exposure of the extra factor could cause serious damage in banks [18].

The usability results [7] indicate that devices used for OTPs still cause problems because users require instructions to use it. Nevertheless, authors [13] argue that the overall usability of 2FA technologies is high and also impart that advanced and more secure technologies aren't necessarily less usable. Conversely, the research [16] has discrepant perspective and argues that the complexity of 2FA methods has a negative effect on its rate of adoption, which is caused by usability. These conflicted arguments can be understood by the conclusion from [9]: "…*system design can significantly impact user behaviour, sometimes in unanticipated ways, which in turn can significantly impact the security of a system*". Justifying the collision, it should be recognised that User-Interface (UI) is an important part of the system and can hugely impact users' behaviour, implying that secure technologies can be less usable but it's not necessarily a rule for all cases.

[2] **token-** term refers to One-Time-Passwords (OTPs) that are generated by dedicated devices or dedicated applications

The present trend of technological evolution and the way researchers are proceeding with development of 2FA methods can be summarised with the quote from [5]: "*…different implementations of the same authentication method will provide very different levels of security*". In essence, methods recently presented in papers use the same theoretical background, but neoteric technology is used. For example, smartphones replaced old-school devices and dedicated applications which are now generating OTPs.

The next section evaluates methods that will keep us au courant[3] with technology.

2.6 Modern Token-Less 2FA

The cutting-edge mobile technology has largely influenced the way people communicate and use information. Smartphones are capable of being multi-purpose and can potentially provide secure 2FA. Because they're essential in our lives, the ability to include them as part of 2FA (i.e. token-less factor) is tremendous.

2.6.1 Mobile-OTPs and QR-Codes

Mobile-OTPs are the present subject of research, and consequently mobile platforms are commonly used in recent developments [19] [20] [21]. Essentially, researches tackled diverse security problems due to rise of high-degree techniques such as Phishing or Pharming and related attacks. Sensitive applications (i.e. e-banking) increasingly prefer more secure authentication alternatives giving a reason to develop improved mobile-OTP methods. Research [21] reviles security properties of mobile-OTP solution that protects against replay-attacks and guessing-attacks, but is defenceless against Man-In-The-Middle (MITM). Consequently, authors [20] deliver similar suggestion, which is additionally secure against MITM, furthermore it validates the previously mentioned quote[4] and demonstrates that different implementations of the same method can provide different security.

Commensurable method [19] indicates security properties similar to methods in [20] [21], however contradistinction was found in testing practices, because their method was tested in practice for a year and validated security assumptions. Importantly, it's the only research in which the solution was tested in a live environment. Deploying and testing an innovative method can lead to great results especially when usability and security factors come into play, and also helps to verify weaknesses and address them in future developments.

2.6.2 QR-Based OTP

Mobile-OTP methods include combinations of SMS-OTPs, for example SMS-to-PC, SIM-authentication with SMS etc. [21]. However, the most renowned are dedicated applications, which use Quick-Response-code (i.e. Google-authenticator). Mobile-based solutions constructed with QR-code can entirely remove the need for the password table which stores long-term secret keys and also is a cost effective solution since many Internet users have smartphones [22].

QR-based solutions bring sui generis[5] advantages from the security and usability perspective. The recognised advantages are: capability of omni-direction[6] readability, error correction capability and support for devices that aren't equipped with QR-reader. Furthermore, QR-code amalgamates three factors: high-data-capacity, reduced-space-printing and high-speed-reading, these factors make mobile-based methods a lot more powerful. Similar researches [23] [24] point-out distinct QR-based

[3] **au courant**- up-to-date in knowledge

[4] **quote-** recall following quote from [5] "…*system design can significantly impact user behaviour, sometimes in unanticipated ways, which in turn can significantly impact the security of a system*"

[5] **sui generis**- unique or very special characteristics

[6] **omni-directional**- all directions are equal, also sending or receiving signals in all directions

solutions, which are highly secure and prevent from password guessing, impersonation, replay-attacks, DDoS-attacks and Phishing-attacks. Additionally, QR-code itself creates a barrier against malicious users because the system requires a prerequisite input of transaction using it and then authorises authentication to generate OTP.

Works [23] [24] proffer methods that are secure but don't make evident the usability properties. Lack of usability measures is a gap that can be tackled in future work with comparative usability study. In fact, [23] indicates that critical look into the practical threats and related analysis are imperative, i.e. usability analysis. Future expansions of 2FA methods can lead to the development of a generic Three-Factor Authentication method that can offer security assurance for protecting classified data.

The latest research reveals that current mobile-based 2FA methods have conceptual weaknesses, because adversaries can capture OTPs or steal private key material for OTP generation [25]. Therefore, exploration of authentication mechanisms that use secure-platform can also be the future work proposal.

3 Conclusions

The logically structured review evaluated findings in theoretical and practical uses. In the literatures, diversified solutions capable of replacing old-school methods were presented, which can also be combined with traditional ID/password approach. So, knowledge was gathered to answer questions from abstract. Outcomes presented can lead to further elucidation of 2FA and the following sections cover the summary of findings, the challenges that 2FA is facing, and future works.

3.1 Summary of Findings

Undoubtedly, technological advances provide an excellent platform for implementing strong authentication methods but also enable intruders to use it against us. Consequently, Internet turned into an environment for exchanging information, and is used to access online services. Online access to resources opens up awareness about security. E-banking needs the highest possible security in order to protect the privacy of their clients. Existing security measures suggest that e-banking systems aren't secure and robust enough to address the security threats and violation attempts.

The literary review highlighted some compelling problems of the Internet and brought to our attention the lack of a comprehensive method that would deal with service concurrency, security, usability, and availability. E-banking services that aren't secured enough can be in danger of cyber-attacks. Impact of such attacks can be disastrous, and can result in being costly and create service downtime. The solution to insecurity is the multi-factor authentication; the extra layer of security can prove to be a successful barrier against cyber-criminals.

The concept of strong authentication isn't adequate, so generally it's referring to the security of 2FA methods and the assurance level that an authentication-token is neither compromised nor circumvented. Section 2.4 revealed that knowledge-based and possession-based authentication-types are primarily used, and biometric-based authentications are eradicating because they're costly and usability problems are prevailing. Similarities in [19] [20] [23] [25] ascertain that possession-based methods are prominent; furthermore, mobile platforms are fundamental in token-less approaches, which is the factor that eliminated old-school methods. (**A1**)[7]

Smartphones and smartcards can potentially provide strong authentication with regards to its implementation. They're capable of protecting tokens, storing password files, OT-password files etc.

[7] **A1**- paragraph implicitly answers Q1 set in abstract

Coalescence of ID/password and smartphone/smartcard methods can form 2FA, which will enhance the security of the system.

Existing mobile-OTPs split into SMS-based and APP-based[8] OTPs. In SMS-based method, SMS is delivered to users with a unique OTP that was generated by the service provider. This method is still used in e-banking, however it's only recommended for services that don't require heavy protection [23]. Furthermore, SMS-OTPs aren't cost effective and can be problematic when mobile-network is overloaded. SMS-based methods are slow, unreliable and expensive, and consequently, these factors tremendously decrease the usability. APP-based methods have the potential and could cure problems of SMS-OTPs. (**A2, A3**)[9]

The literature review clearly delineates that researchers concentrated on APP-based methods because they're fast, secure and reliable, and can potentially suit e-banking. Conversely, APP-generated OTPs, rely on pre-shared secrets where the distribution process of pre-shared secrets is a valuable attack vector [25]. Furthermore, generated QR-code can be captured if the device contains attacker's software, in consequence the unique OTP will be in hands of an attacker. Moreover, existing mobile-based schemes have conceptual weaknesses, because attacker can possibly steal private QR-code for OTP generation [25]. Contrastingly, QR-codes protect from malicious users, increasing the security, therefore should be used in APP-based methods [23] [24]. This leads us to challenges and future work sections. (**A2, A3**)

3.2 Challenges

The major challenge is to implement a 2FA solution that has high usability and security, easy deployment and low running costs. Nevertheless, the trade-off between usability and security causes various problems for users and developers. Findings emphasise that advanced technology ameliorated methods in terms of security but the lack of real world feasibility study works against the implementation of them as the factors by which users select their method are unknown. The possible cure can be a comparative usability study of mobile-based solutions, which will verify factors that influence a selection of methods.

The importance of UI has been pointed-out in literature review [9]. It's evident that implementation of usable UI is a challenge in any system, and in fact UI is the preeminent factor that influences usability. In addition, developers should face the challenge of delivering UI that will eliminate the need for instructions in order to use the system.

3.3 Future of 2FA

APP-based authentication was verified to be very secure, but it was argued that there are conceptual weaknesses [25]. The weaknesses are hardware-oriented showing that mobile platforms have limitations which are caused by lack of support for a secure UI and platforms aren't freely programmable. Future implementations on secure hardware could eliminate the integral weaknesses of existing 2FA methods.

Finalising Section 3, future research should critically analyse the practical threats against security and this could lead to the development of a generic Three-Factor authentication method.

[8] **APP-based**- term relates to dedicated applications available on smartphones, piece of software only

[9] **A2, A3**- paragraph implicitly answers Q2 and Q3 set in abstract

References (IEEE)

[1] A. Adams and M. A. Sasse, "Users Are Not The Enemy," *Communications of the ACM,* vol. 42, no. 12, pp. 41-46, 1999.

[2] M. Mannan and P. C. Oorschot, "Security and Usability: The Gap in Real-World Online Banking," *NSPW'07,* pp. 1-14, 2008.

[3] M. Matthews , "Where next for account aggregation?," *International Journal of Bank Marketing,* vol. 24, no. 2, pp. 133-138, 2006.

[4] B. Davaanaym, Y. S. Lee, H. J. Lee, S. G. Lee and H. T. Lim, "A ping pong based one-time-passwords authentication system," *NCM '09 on INC, IMC & IDC,* pp. 574-579, 2009.

[5] S. Z. Idrus, E. Cherrier, C. Rosenberger and J.-J. Schwartzmann, "A Review of Authentication Methods," *Australian Journal of Basic and Applied Sciences,* vol. 7, no. 5, pp. 96-107, 2013.

[6] R. E. Smith, Authentication: From Password to Public Keys, Boston: MA: Addison-Wesley, 2002.

[7] C. S. Weir, G. Douglas, M. Carruthers and M. Jack, "User perceptions of security, convenience and usability for ebanking authentication tokens," *CCIR,* vol. 28, no. 1-2, pp. 47-62, 2009.

[8] D. Jyoti and R. Kumar, "Review of Security Analysis and Performance Evaluation of an Enhanced Two-Factor Authenticated Scheme," *International Journal of Electrical,* vol. 3, no. 1, pp. 218-22, 2014.

[9] S. Akram, M. Misbahuddin and G. Varaprasad, "A Usable and Secure Two-Factor Authentication Scheme," *Information Security Journal: A Global Perspective,* vol. 21, no. 4, pp. 169-182, 2012.

[10] Z. Moshe and E. Zippy, "Identification and Authentication: Technology and Implementation Issues," *Communications of the Association for Information Systems.*

[11] D. Besnard and B. Arief, "Computer security impaired by legitimate users," *Computers and Security,* vol. 23, no. 3, pp. 253-264, 2004.

[12] J. Johnston, J. H. Eloff and L. Labuschagne, "Security and human computer interfaces," *Computers and Security,* vol. 22, no. 8, pp. 675-684, 2003.

[13] E. De Cristofaro, H. Du, J. Freudiger and G. Norcie, "A Comparative Usability Study of Two-Factor Authentication," *CoRR,* pp. 1-10, 2013.

[14] L. O'Gorman, "Comparing passwords, tokens and biometrics for user authentication," *IEEE,* vol. 91, no. 12, pp. 2021-2040, 2003.

[15] B.-K. Jeong and T. E. Yoon, "An Empirical Investigation on Consumer Acceptance of Mobile Banking," *Sciedu Press- ISSN,* vol. 2, no. 1, pp. 31-40, 2013.

[16] E. T. Cheng, D. Y. Lam and A. C. Yeung, "Adoption of Internet banking: An empirical study in Hong Kong," *Decision Support Systems,* vol. 42, no. 3, pp. 1558-1572, 2006.

[17] B. Schneier, "Two-Factor Authentication: Too Little, Too Late," *Communications of the ACM,* vol. 48, no. 4, 2005.

[18] W. Go, K. Lee and J. Kwak, "Construction of a secure two-factor user authentication system using fingerprint information and password," *Springer Science+Business Media, LLC,* vol. 25, pp. 217-230, 2012.

[19] Y. Huang, Z. Huang, H. Zhao and X. Lai, "A new One-time Password Method," *International Conference on Electronic Engineering and Computer Science,* pp. 32-37, 2013.

[20] K. Bicakci, D. Unal, N. Ascioglu and O. Adalier, "Mobile Authentication Secure Against Man-In-The-Middle Attacts," *The 11th International Conference on Mobile Systems and Pervasive Computing,* pp. 323-329, 2014.

[21] D. v. Thanh, I. Jorstad, T. Jonvik and D. v. Thuan, "Strong authentication with mobile phone as security token," *IEEE 6th International Conference on Mobile-Adhoc and Senso-Systems,* pp. 777-782, 2009.

[22] K.-C. Liao and W.-H. Lee, "A Novel User Authentication Scheme Based on QR-Code," *Journal of Networks,* vol. 5, no. 8, pp. 937-941, 2010.

[23] N. Harini and T. R. Padmanabhan, "2CAuth: A New Two Factor Authentication Scheme Using QR-Code," *IJET,* vol. 5, no. 2, pp. 1087-1094, 2013.

[24] Y. S. Lee, N. H. Kim, H. Lim, H. Jo and H. J. Lee, "Online Banking Authentication System using Mobile-OTP with QR-code," *Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International-Conference,* pp. 644-648, 2010.

[25] A. Dmitrienko, C. Liebchen, C. Rossow and A.-R. Sadeghi , "Security Analysis Of Mobile Two-Factor Authentication Scheme," *Intel Technology Journal,* vol. 18, no. 4, pp. 138-161, 2014.

Words Count: 3999 (excludes cover page and footnotes)

--End of literature review--