The Case for Two-Factor Authentication- Evidence from a Systematic Literature Review

Completed Research Paper

Pengcheng Wang Richard Baskerville

Two-factor authentication uses any combination of an authentication modality or the combination of multiple features of different authentication modalities, and it has been argued for many years that it can protect against the pitfalls of the password and PIN only authentication system, however, there is no empirical evidence to support such argument. A systematic review of studies of two-factor authentication was conducted, and 38 studies from ABS/Inform and EBSCOhost were analyzed in detail. The review investigates what is currently known about the benefits and limitations of two-factor authentication and How additional authentication factors affect security risk in relation to security costs. We found no strong evidence to support the assumption that two-factor authentication has superior performance. We did, however, find strong evidence that it can bring many unexpected risks. For future research, we need to increase both the number, the quality of studies and the critical stance of research on two-factor authentication.

Keywords: two-factor authentication, information security, systematic literature review.

Introduction

Security is critical for an information system (IS). The information security threats include natural and human-made disasters, errors by employees, viruses, hackers, etc.(Karen D. Loch, Houston H. Carr, & Merrill E. Warkentin, 1992). To reduce the information security threats, organizations tend to rely on technology solutions or employees' compliance with information security policies. Many organizations consider employees as the weakest link in information security (Bulgurcu, Cavusoglu, & Benbasat, 2010).

Nevertheless, we assume that it is more effective to implement a more sophisticated and comprehensive authentication scheme to compensate for man-made disasters, human errors and hacker threats (Cheong, Ling, & Teh, 2014; Connie, Teoh, Goh, & Ngo, 2004; Kumari & Khan, 2014; Yang, Wong, Wang, & Deng, 2008). An example of such increased complexity is replacing a single-factor authentication-based system with a multi-factor authentication-based system. In general, authentication is the information security method that intends to protect against any illegitimate access to an individual device or data server (Dasgupta, Roy, & Nag, 2016). The most widely adopted authentication method is the password or personal identification number (PIN) based single-factor authentication. Despite this wide adoption, many researchers find weaknesses in this method (Cheong et al., 2014; Connie et al., 2004; Kumari & Khan, 2014; Yang et al., 2008). For example, the password or PIN can be lost, forgotten, illicitly acquired by direct observation, hacked by dictionary attacks or an online guessing attack. Many suggest that a two-factor authentication system can insure against the pitfalls of single-factor authentication. Consequently, using a combination of multiple factors has become a prevalent trend on the assumption that it provides more secure, more resilient, and more robust access to digital systems. It is widely assumed that security for a password-protected system will be improved by expanding the access control to include two-factor authentication. Intuitively, adding an additional factor(s) to existing single-factor authentication system is an obvious

solution. However, our research suggests that this assumption is both unproven and questionable. In contrast, our study finds that the evidence in the literature points to many security weaknesses in various two-factor authentication schemes. Also, adding additional authentication factor can cause operability difficulties such as high computing power requirement, low reliability and high operating cost. Therefore, our research question is:

How do additional authentication factors affect security risk in relation to security costs?

A superficial review of the literature suggests there may be a dearth of research that supports the assumed efficacy of two-factor authentication. Accordingly, we undertook a systematic literature review on this topic. Our objectives are to evaluate, synthesize and present the empirical findings on two-factor authentication to date and provide an overview of the topics that have been studied. We will use these findings and implications to suggest future research directions.

This study finds a clear growth in interest in two-factor authentication. More than half of the relevant research articles were published after 2013. Missing is strong empirical evidence that shows how two-factor authentication can deliver superior performance for information security. In fact, the available evidence indicates the opposite: that adopting two-factor authentication brings a lot of unexpected risks.

Authentication Challenges

Authentication is an information security method to protect against any illegitimate access to digital devices and data servers (Dasgupta et al., 2016). As a baseline, we will briefly review research on the security effects of improving one factor authentication. Passwords are a prevalent and traditional form of one factor authentication.

The problem of poor password selection and hygiene is well-known. Strong passwords are long, random, contain, multiple character types, and are unique. Strong passwords introduce entropy into intrusion process. It takes more work to attack such passwords. But we know that, without improving the password-setting process, people will choose simple, easily cracked passwords. For example, Hunt 2011[1] analyzed 37,608 passwords revealed as part of a Sony breach. He found that half of these passwords were less than eight characters in length, and only about one percent used alphanumeric characters.

Two-factor authentication uses any combination of an authentication modality or any combination of multiple features of different authentication modalities. In general, the two-factor authentication uses a combination of features taken from:

- *The Knowledge Factor, what we know, such as a password*
- *The Possession Factor, what we have, such as a smart card*
- *The Inherent Factor, what we are, such as a fingerprint*

Many researchers claim that the two-factor authentication can insure against the pitfalls of single-factor authentication, for example, the Man in the Middle attack and Phishing (e.g., Kiljan, Simoens, De Cock, Van Eekelen, & Vranken, 2016; Sarel & Marmorstein, 2006; Yoo, Kang, & Kim, 2015). They believe that using a combination of multiple features is an ongoing trend to provide secure, resilient, and robust access to preserve the legitimacy of the digital users. That is, the use of two-factor authentication for information security is an improvement.

Others are less confident. For example, the most common scheme for two-factor online banking authentication combines the traditional password process with an SMS challenge code sent to the user's mobile phone. The user must possess this challenge code to complete the login process. Schneier (2005) explains how such a simple two-factor (or two-channel) approach does little to prevent Man in the Middle attacks. Such approaches can still be easily defeated by lax security practices, such as storing plaintext passwords on an unencrypted mobile phone. If the phone is stolen, the attacker controls both factors, and

[1]https://www.troyhunt.com/brief-sony-password-analysis/

the users even suffer higher risk due to fact that the bank usually allows higher transaction amounts with two-factor authentication.

We question whether introducing a second factor in the authentication process (such as a token) is more effective than hardening one factor (such as improving password practices). With this background in mind, we set about a systematic literature review to determine what we know about the efficacy of two-factor authentication.

Systematic Literature Reviews Methodology

The notion of a systematic literature review first arose in the evidence-based practices of medicine. A systematic literature review synthesizes "… research in a systematic, transparent and reproducible manner to inform policy and decision-making about the organization. … Systematic reviews differ from traditional narrative reviews by adopting a replicable, scientific and transparent process, in other words a detailed technology, that aims to minimize bias through exhaustive literature searches of published and unpublished studies and by providing an audit trail of the reviewers decisions, procedures and conclusions." (Tranfield, Denyer, & Smart, 2003, p. 209)

In this study, we are interested in the efficacy of two-factor authentication and its evidence of this efficacy in the research literature. Two-factor authentication has been extensively studied in computer science and information system fields, and many studies have addressed same security challenges by using *different* two-factor authentication approaches. Many other studies have tried to manage the security challenges by using the *same* two-factor authentication approaches, but while using an improved or modified algorithm. These similar but comparable studies provide a perfect environment in which to apply a systematic literature review for comparing, interpreting and translating the key concepts in the selected articles.

Data Collection Process

Two databases were selected: the ABI/Inform Collection and EBSCOhost Database, and our search query is: (1) "two factor authentication"; (2) "two-factor authentication"; (3). 2FA; (4) "dual factor authentication";(5)"dual-factor authentication"; (6) "two-stage authentication"; (7) "two stage authentication"; (8) "two-step authentication"; (9)"two step authentication"; (10) "two-factor verification"; (11) "two-factor verification"; (12) "multi-factor authentication" ; (13) "multi factor authentication"; (14) "multiple factor authentication"

Different criteria were applied in the different search and analysis stages in this review. First, the time frame for this systematic review is from 2000 to 2016. The article must be written in English and published in a peer-reviewed academic journal. Second, studies were eligible for inclusion in this review only if they focus on two-factor authentication. Third, as our research questions are concerned with two-factor authentication; articles will be excluded if the research focus is on single or multiple authentications (more than two factors). The selected articles must focus on the development of any combination of two-factor authentication. Finally, given that our focus is on a search of the empirical evidence that evaluates the effectiveness of two-factor authentication in general, papers without a rigorous research design (e.g., an editorial note or an industry survey), and papers based merely on expert opinions were excluded. Excluded also from the search were books, conference, news, editorials, workshop sessions, discussion, comments, etc. In this initial stage search, 220 and 662 articles were identified in ABI/Inform and EBSCOhost respectively. All results were exported separately to an Endnote database for further analysis.

Based on an analysis of the title, keywords and abstract, we eliminated all irrelevant articles, leaving 63 articles were brought forward to a detailed analysis. We performed a detailed analysis of all 63 articles and classified the selected articles into different groups. Since our study focuses on synthesizing and evaluating any new or improved two-factor authentication scheme, we further excluded the papers that lacked an appropriate, rigorous, empirical research design. This exclusion left 38 articles.

We used the Nvivo to analyze and synthesize the 38 selected articles creating a table in Microsoft Word for each article. These tables supported comparison of the articles' research questions/objectives and proposed solution(s). The detailed findings are discussed in the finding section.

Findings

In this section, we discuss the overall evaluation and the detailed evaluation results that regard the strength of the evidence of selected articles.

Based on these 38 relevant articles, we can see a trend of rising attention to two-factor authentication. Nineteen (50%) of the selected articles were published after 2013. Among the 38 articles, 12 (32%) are mainly based on adding biometric factors such as fingerprint and palm print to a password-only authentication scheme. The rest of the articles (68%) focus on improving system security by adding a possession factor (such as a smart card or a digital key). Among 38 selected articles, the smart card and password are most studied two-factor authentication scheme, followed by fingerprint, digital key, gait recognition, face recognition, radio frequency identification, one-time password and palm print.

We had expected to find evidence in the literature that would guide us in deciding which of the available authentication factors worked reliably together in which situations. It was somewhat surprising to find that nearly all of the related studies dealt with weaknesses in the various known factors. Some studies examined these weaknesses, and we designated the knowledge from these studies as *problem-centered weaknesses*. Many of these studies not only examined such weaknesses, but also proposed solutions, and we designated the knowledge from these studies as *solution-centered weaknesses*. In the selected studies, problem-centered weaknesses arose from studies of compromises of the available factors. Solution-centered weaknesses arose from the development of improvements related to the available factors.

Theme 1. Problem-centered Weaknesses in Authentication Factors

Password Weaknesses: Password or PIN authentication is widely used on its own in single-factor settings. Not surprisingly it is also commonly used as one of the two factors in two-factor authentication. Given its prominence, password compromises are well studied. Many studies indicate that passwords or PINs can be lost, forgotten, illicitly acquired by direct observation, and hacked by dictionary attacks or online guessing attacks (Cheong et al., 2014; Connie et al., 2004; Kumari & Khan, 2014; Yang et al., 2008). Such attacks are made easier when users are permitted to choose weak passwords. Password or PIN-based authentication usually requires the servers to maintain a verifier table to match the inserted password with the stored password before granting access (Kumari & Khan, 2014). If the verifier table is exposed, it can be compromised by various automated methods, even while still encrypted. In addition, many users practice poor security hygiene by using the same PINs or passwords for many, if not all, of their accounts. Compromise of one of their accounts can lead to compromise of their other accounts (Wang, Wang, Wang, & Qing, 2015).

Two-factor authentication is supposed to provide more secure and robust ways to protect sensitive information than with passwords alone. Password or PIN authentication has well-known weaknesses. However, our systematic literature review turns up findings that suggest the other possible factors in two-factor authentication also suffer many risks. These will be discussed below.

Weaknesses in biometric-based two-factor authentication

Template compromises: Adding biometric factors into authentication scheme has inherent advantages. A biometric based two-factor authentication system does not require the users to carry the physical key or memorize a password (Cheong et al., 2014). However, these inherent characteristics also bring challenges. Ntantogian, Malliaros, and Xenakis (2015) admit that biometric-based two-factor authentication systems require very high protection for the extracted template. Due to impersonation attacks, users' immutable biometric templates will be useless if the templates are stolen. The biometric templates from users are

unchangeable, and the new templates cannot be assigned when compromised (Pang, Andrew, & David, 2007). Many researchers indicate that it is critical to create a *concealed* biometric-based two-factor authentication (Ma, Wang, Li, Zhang, & Huang, 2014; Pang et al., 2007). The sensitive nature of biometric data has alarmed the public's concern about privacy issues (Connie et al., 2004). Khan et al. (2011) find that, if users' biometric data leaks to unauthorized party, the data could be misused. For example, unauthorized users may use the stolen data to log into users' accounts in multiple accounts where the same biometric templates exist. It can result in lost integrity for the whole security stem. The only remedy is to replace the stolen data by other biometric templates. However, users only have limited number of biometrics traits. Also, Ma et al. (2014) find that biometric data cannot be kept in explicit form; it must be converted into encrypted form. If the biometric template needs to be stored on a portable device, such as a mobile phone or laptop, it suffers a higher risk of theft and malware. The users become more vulnerable to security and privacy threats, not less.

Costliness: Compared with other authentication systems, a biometric-based authentication system is expensive. The high implementation cost is another concern for the companies who want to adopt a biometric-based two-factor authentication system. The use of multiple biometric measurement and storage devices will impose significant additional costs. For example, designing a new and more sophisticated user interface affects usability and additional management complexity is generated (Cheong et al., 2014; Connie et al., 2004; Lat, Bondoc, & Atienza, 2013).

Reliability: In addition, the biometric authentication suffers from high false acceptance rates and high false rejection rates (Pang et al., 2007). The biometric features of the same subject cannot be extracted exactly same, and the system has to tolerate a certain level of data noise. As a result, the authentication system may fail before the user can get access (Ntantogian et al., 2015). Natantogian et al. (2015) further indicate that the encrypted biometric template can increase even more intra-variance, resulting in even higher false rejection rates and false acceptance rates. Therefore, system owners must figure their optimal balance point between security and performance.

Weaknesses in Possession Factor Authentication

Smart-card compromise: In two-factor authentication literature, smart-card-based two-factor authentication is the most highly studied. This authentication method requires the user to carry a physical chip-enabled device, and it requires the users to insert it into a reading device before accessing his/her account. The smart card can provide extra security layers, but its stored secret information can be revealed with techniques such as power analysis, reverse engineering, fault injection attacks, and other kinds of side-channel attacks (Islam & Khan, 2014; Wang et al., 2015). Compared with biometric based authentication, the inherent disadvantage of smart card based authentication is that the system is very vulnerable to impersonation attacks. It is hard for the system to distinguish the legitimate or malicious access because both the smart card and the password can be stolen (Chaudhry, Naqvi, Shon, Sher, & Farash, 2015). Chaudhry et al. (2015) concludes that the smart-card-based two-factor authentication is unsuitable for practical deployment if the server cannot distinguish legitimate from malicious users' access.

Impersonation: Impersonation attacks are highly related to the lost/stolen smart card. If the smart card is lost or stolen, there is no effective way to prohibit it from misuse (Kumari & Khan, 2014). The confidential information stored in the smart card can be extracted by an external device that physically monitors its powers consumption. There are also other kinds of side-channel attacks if the end users' authentication request cannot be transmitted via a secure channel during the login and key agreement protocol (He, Kumar, & Khan, 2013; Wei, Liu, & Hu, 2014). A smart card is also vulnerable to the password guessing attack, especially when it is stolen. Chaudhry et al. (2013) find that an adversary can get the password with the help of certain off-line methods unless the server is able to distinguish a valid smart card from a lost one. They argue that the authentication system should provide a proper revocation method to handle a lost smart card. In addition, the compromise of information stored in the smart card can also reveal users' identities. Many studies indicate that the user's privacy protection is an important requirement when implementing a

smart card based authentication system (Chang, Lee, Lin, & Liu, 2015; Dasgupta et al., 2016; Gupta & Dhar, 2016; Jiang et al., 2016; Kumari & Khan, 2014). Issuing a new or replacement smart card can dramatically increase system cost, and additional equipment is also needed to read and store data into smart card (Gupta & Dhar, 2016).

Token weaknesses: Token based two-factor authentication is another popular method in this category. The token can be a hardware, software, mobile phone, or cloud-based QR code (Cheng, 2011). Cheng (2011) found that such tokens suffer several drawbacks, such as poor token interoperability, poor inter-system compliance, high hardware and support cost, and poor portability. Token based security suffers risks similar to smart cards if the token is stolen or lost. It is not very convenient for the end users because it requires the user to have specialized hardware that may need to be replaced if it has unreplaceable battery or restrictions on the number of uses (Lat et al., 2013). Besides that, Ku et al. (2013) find that some one-time use tokens only use a 64-bits password. It makes the authentication system vulnerable to offline password guessing attacks (He et al., 2013; Yunlim Ku et al., 2013; Y. Ku et al., 2013).

Theme 2. Solution-Centered Weaknesses in Authentication Factors

According to the previously synthesized findings, we find that two-factor authentication can be problematic when both factors have security issues. Not surprisingly, much of the existing research in the selected articles involves: first, highlighting one of the serious problems with two-factor authentication and second, proposing a new method for two-factor authentication that improves the existing approaches. In the following section, we discuss the issues that are indirectly evidenced by the proposed security solutions offered in the selected articles.

Biometric based two-factor authentication

Compared with other kinds of two-factor authentication, the biometric-based two-factor authentication does not require the user to carry a physical key or memorize additional knowledge (Cheong et al., 2014). However, many selected articles indicate how biometric-based two-factor authentication has three major issues: a severe privacy protection requirement, high implementation and operation costs, and both high false rejection rates and high false acceptance rates.

Lack of Biometric Cryptosystems: With respect to the severe privacy protection requirement, Hoang et al. (2015) proposed using a biometric cryptosystem as an approach to maintaining the security and privacy of the biometric system. Their approach allows the user to store this sensitive data on their mobile devices instead of the system server. They propose a gait based two-factor authentication system that verifies users' legitimacy. The system consists of a stored cryptographic key that is biometrically encrypted by gait templates collected from a mobile accelerometer. This pre-collected gait template will be used only once and discarded after authentication process completed. The Hoang et al. (2015) solution aims to solve the biometric privacy issue and protect users' sensitive data from any server compromise. Because the system collects the gait template without any user interactions, it is highly convenient. However, Hoang et al. (2015) admit that gait is less discriminating and more noisy than other biometric modalities such as scanning the iris, fingerprint, face, etc. They report an average false rejection rate over 15%; quite high compared with other methods. In addition, the pre-collected gait template can only be used once. Because the system requires enough time to collect a new gait template after one-time use, the system will not support frequent access authentication during short periods

Lack of Hash Functions: Another stream of literature proposes the use of hash functions to encrypt the extracted biometric templates (Connie et al., 2004; Khan et al., 2011; Ntantogian et al., 2015; Pang et al., 2007). Ntantogian et al. (2015) proposed a Biohash technique to protect users' data. The Biohash technique can transform biometric template to a noninvertible bit stream using the Biohash algorithm and a user token. Ntantogian et at (2015) claim that this token and biometric based two-factor authentication scheme is more secure because the individual user must not only provide a unique token for authentication, but also require

authentication by a biometric feature. In addition, Pang et al. (2007) also propose tokenized biometric data as a measure to prevent server comprises. If the stored token-based biometric data is compromised, the system will issue a new tokenized biometric template.

Users Have Only a Limited Number of Biometric Traits: Because all of the biometric templates are tokenized, the system can convert the same biometric trait, such as the same fingerprint, into different bit streams through a hash function (Connie et al., 2004). Further, users can combine the same biometric trait with different tokens for use with multiple accounts. In this way, it reduces the systematic risk that might otherwise occur if a user's biometric data are stolen. By combining the token and the biometric template through a hash function, we can remedy the weakness of a biometric-based authentication system that depends on the users' limited number of biometrics traits.

High Implementation and Operating Costs: With respect to cost reduction, Hoang et al. (2015) is the only study clearly concern about cost reduction. Hoang et al. (2015) claim gait based two-factor authentication takes advantage of a fuzzy commitment scheme, so their two-factor authentication only requires small storage space and low computational complexity. However, as we indicate in the previous section, computing power, and storage space are only part of the full system, and the multiple biometric measurement devices, such as fingerprint reader, face traits scanner, could cost a lot. Therefore, we argue that Hoang et al. (2015)'s cannot change the fact that the biometric based two-factor authentication could be the most expensive system comparing with other kinds of two-factor authentication systems.

High False Rejection and Acceptance Rates: With respect to reducing false rejection rate and false acceptance rate, no study in our selected articles offered a means to effectively reduce the false rejection rate and false acceptance rate. There is no evidence show that biometric-based two-factor authentication system can achieve the same accuracy as other kinds of two-factor authentication system. For example, smart card based two-factor authentication can deliver close to 0% false authentication indications.

Possession Based Two-Factor Authentication

Possession based two-factor authentication especially smart card based are most studied. Possession based authentication system requires the user to carry a physical key or token to access the system, and the physical keys or token could be a smart card or mobile device that can generate or receive one-time use access codes. Many selected articles indicate that a possession-based two-factor authentication system can be very vulnerable when the smart card or one-time password token is stolen. Protecting the information stored in the smart card or mobile device is the major challenge.

Lack of Smart Card Encryption: The information stored in the smart card cannot be in plaintext. Kim et al. (2014) indicate the hackers could use all the information stored in the smart to attack users' accounts, so encrypting the information stored in the smartcard and realizing user anonymity are critical. Several techniques were proposed in the selected articles. Juan et al. (2014) claimed that elliptic curve cryptosystem could help smart card based two-factor authentication resist impersonation attacks, internal attacks, internal offline guessing attacks, server spoofing attacks, etc. However, the author did not explain clearly how the elliptic curve cryptosystem works and how they use it in their proposed authentication system. Jiang et al. (2016) also used elliptic curve cryptography to design an untraceable two-factor authentication system. They claim their proposed authentication method could make up for the missing security features necessary for real-life performance. However, Jiang et al. (2016) only perform a security analysis to evaluate their authentication method, and they did not use any empirical data. Their findings and arguments may not hold in a real-world situation. Chaudhry et al. (2015) and Arshad et al. (2015) also use the elliptic curve cryptography technique to achieve user anonymity. However, these studies also neglect the use of a simulation or experiment to support their findings. The evidence to support their arguments is weak.

Lack of User Anonymity: Another stream of literature uses dynamic ID-based techniques to achieve user anonymity and un-traceability (Cao & Zhai, 2013; Chang et al., 2015; Islam & Khan, 2014; Wang et al.,

2015). Wang et al. (2015) claimed that the dynamic ID-based technique is simpler and more robust. Dynamic ID techniques can help the authentication system achieve security and privacy at the same time by using a public-key encryption with proper padding mechanisms. Chang et al. (2015) designed a two-factor authentication scheme and they use a dynamic ID-based technique that eliminates all constant parameters from the user's messages such that any two messages are independent and indistinguishable. Chang et al. (2015) claim their proposed smart-card-based two-factor authentication can achieve user anonymity and resist various attacks like impersonation attacks, stolen verifier attacks and lost smart card attack. Islam et al. (2014) and Cao and Zhai (2013) also argue that the dynamic ID technique can enhance system security. Unfortunately, none of above articles discloses empirical tests of their authentication systems, e.g., using simulations or experiments. It is unknown how their authentication would work in a real work situation.

Demanding Computer Power and Operating Complexity: A one-time password token is another stream aimed at developing a possession-based two-factor authentication. For this purpose, Cheng (2011) creates a new cipher system called Rubbing Encryption Algorithm (REAL). This authentication system can generate a ciphertext REAL image in which is a type of encrypted one-time password. The user can decrypt the REAL by laying the hardware token over the REAL image on the screen (i.e., scan the token on the screen) to get the one-time password. The system does not require the user to memorize the decryption key, so the REAL image can contain a long and complicated encryption key that enhances the overall system security. In addition, the authors claim that the REAL does not use a complicated mathematic operation. It only requires a small level of computing power to operate the system, so it can also reduce the implementation cost. In addition, Y. Ku et al. (2013) use graphical one-time password technique to create two-factor authentication to protect users from shoulder surfing attacks, man in the middle attacks and other phishing attacks. Their authentication method utilizes users' memory by implementing a story-telling mechanism in which users are required to create a *pass* image portfolio, and users need to identify the pass images from among fake images before entering next authentication process. However, the authors did not provide any empirical evaluation in their study. The superior performance of their proposed authentication scheme is yet to be established.

Discussion

This systematic literature review elaborates previous research into two-factor authentication by focusing on the meaning of existing empirical research in the area to current practice. There is a predominant assumption that two factors will provide better security than one factor (Cheong et al., 2014; Connie et al., 2004; Kumari & Khan, 2014; Yang et al., 2008). However, the research literature shows that these second factors are as rife with weaknesses as passwords. They are often costly, complicated to use, and open new avenues for compromise. Based on our systematic literature review, we found there is no strong empirical evidence to support the argument that two-factor authentication can provide an effective IS security solution.

First, the effectiveness of two-factor authentication is hard to measure because of the inconsistent evaluation method found among all selected articles. Experiments, simulations, security analysis, and cryptanalysis are the most common approaches to evaluating authentication performance. Due to the fundamental difference in these evaluation methods and measurements, it is difficult to compare the performance of different authentication methods directly, and there was not sufficient data to determine which authentication method is better and under what conditions.

Second, there is no strong evidence to support the argument that two-factor authentication can mitigate the risks from the human errors and hacker attacks. Adding additional factors can provide extra security layers, but this study finds that such additional factors can also bring a lot of unexpected risks. Also, none of the selected articles examined the performance of their proposed security scheme in real-world settings. The research results may be biased due to an underestimation of the complexity of human behaviors. For example, the smart-card based authentication based security solution requires the users to secure the smart

card from loss and reporting the loss immediately. If the users fail to comply with the security policy, they would be *more* vulnerable to security threats, especially where higher transaction allowances are allowed with smartcard.

Finally, the results of our systematic literature review of two-factor authentication yields a litany of weaknesses found in the available authentication factors. Most researchers are concerned about the ease of compromise in one or more of these factors. While much of the work aims to improve the security and reliability of these diverse authentication factors, it collectively raises questions about two-factor practices. In other words, are two weak factors really better than one strong one? Considering the additional cost (i.e. high computer cost and extra hardware) and low reliability (i.e. low type II error but high type I error), the answer is unknown and the practice is questionable. Clearly, there may be circumstances in which the adoption of two-factor authentication could well be misguided. It may introduce expensive, complex, user-unfriendly technologies that only deliver the illusion of improved security.

Future research agenda

First, the current two-factor authentication literature lacks a consistent performance evaluation method. We recommend future research is needed that relies more heavily on experiments or simulations to consistently evaluate the performance of these authentication systems. Experiments and simulation methods use empirical data to generate consistent measurements, such as false rejection rates, false acceptance rates and system processing time. Shadish et al. (2001) suggest that experimental results are more generalizable, and such methods are best to investigate causal effect phenomena.

Second, all the selected articles use either lab experiments or simulations as the sole research method. Lab experiments and simulations may underestimate the complexity of human behaviors. As the previous research points out, many organizations consider employees as the weakest link in information security (Bulgurcu et al., 2010). Thus, we recommend more field research that examines practical performance of two-factor authentication in the real-world, naturalistic settings (Lincoln & Guba 1985).

Last, we found that most of the selected articles were concerned with smart card-based two-factor authentication, and this basis leaves uncertainty about the effectiveness of other kinds of two-factor authentication. From the available smart card-based, two-factor authentication-related research, we found lost smart card risk is unavoidable. This lost smart card attack can make this kind of authentication very vulnerable. Thus, we recommend more diverse two-factor authentication studies in the future.

Limitations

It is likely that there are other studies about two-factor authentication that we have not included. Both ABS/Inform and EBSCOhost are well-developed and comprehensive. While it is likely we have the most prominent studies, it is not exhaustive. For example, we did find some two-factor authentication studies that were mentioned in the selected articles but were not included in the search results. This study only included refereed journal papers that dealt with the artifacts comprising two-factor authentication. Survey papers, expert opinions, conceptual papers were not included. Accordingly, the research findings may not reflect the entire literature of two-factor authentication. Third, this study is interpretive research. While both authors were involved in the development process, one author performed the systematic review including article selection, coding, and evaluation. These research findings are subjective, not objective.

Conclusion

In this study, we identified 220 and 662 studies from ABS/Inform and EBSCOhost respectively, of which 38 studies were analyzed in detail. Among these 38 selected articles, smart cards and passwords are most studied of the two-factor authentication schemes, followed by fingerprints, digital keys, gait recognition, face recognition, radio frequency identification, one-time-use passwords and palm prints.

Implementing two-factor authentication can add additional security layers. However, it also brings additional risks. Biometric-based two-factor authentication system does not require the users to carry the physical key or memorize a password, but this kind of authentication requires using and storing sensitive data. This inherent disadvantage makes the system very vulnerable to privacy threats. Also, the biometric features of the same subject cannot be extracted exactly same way twice. The system must tolerate a certain level of noise in the data, requiring the system to have a higher tolerance for variance. This tolerance concomitantly results in low accuracy rates and high implementation costs. In contrast, smart-card-based authentication systems have very high accuracy rates, but if the smart card is lost or stolen, the system could be even less secure than a single-factor authentication system. Hackers can get the information stored in a smart card through side channel attacks, making the system very vulnerable to impersonation attacks. Smart-card-based two-factor authentication systems struggle to distinguish the legitimate access from malicious access. It makes the system less attractive for practical deployment.

This study investigated the efficacy of two-factor authentication. There is a definite lack of empirical evidence to support the assumptions that a two-factor authentication scheme delivers superior security compared to a strong single-factor scheme. There are several reasons for this finding. There is an important need for developing a universal authentication performance evaluation standard. The present constellation of diverse performance evaluation methods and measurements makes the various, existing research findings difficult to comparable. There are no research data that deal with optimally-paired two factor authentication designs. Instead, many of the selected articles used cryptanalysis and security analysis methods as proof-of-concept for artifacts. These kinds of methods do not use any empirical data, leaving unknown their practical performance in real-world authentication systems. It is unclear whether their findings are suitable for practical deployment.

For the future research, the clear finding of the review is that we need to increase both the number and the quality of studies on two-factor authentication. Despite its widely-accepted assumption as an advanced security practice, few researchers have focused on two-factor authentication itself; choosing instead to focus on particular factors: technologies like smart cards and fingerprint scanners. Future research on two-factor authentication will be not only important, but critical for the security of the digital age.

Acknowledgments

I would like to thank the associate editor and the reviewer for the insightful comments on the earlier version of this manuscript.

References

Arshad, H., Teymoori, V., Nikooghadam, M., & Abbassi, H. (2015). On the Security of a Two-Factor Authentication and Key Agreement Scheme for Telecare Medicine Information Systems. *Journal of Medical Systems, 39*(8). doi:10.1007/s10916-015-0259-6

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS. *MIS Quarterly, 34*(3), 523-A527.

Cao, T. J., & Zhai, J. X. (2013). Improved Dynamic ID-based Authentication Scheme for Telecare Medical Information Systems. *Journal of Medical Systems, 37*(2). doi:10.1007/s10916-012-9912-5

Chang, I. P., Lee, T. F., Lin, T. H., & Liu, C. M. (2015). Enhanced Two-Factor Authentication and Key Agreement Using Dynamic Identities in Wireless Sensor Networks. *Sensors, 15*(12), 29841-29854. doi:10.3390/s151229767

Chaudhry, S., Naqvi, H., Shon, T., Sher, M., & Farash, M. (2015). Cryptanalysis and Improvement of an Improved Two Factor Authentication Protocol for Telecare Medical Information Systems. *Journal of Medical Systems, 39*(6), 1-11. doi:10.1007/s10916-015-0244-0

Cheng, F. (2011). Security Attack Safe Mobile and Cloud-based One-time Password Tokens Using Rubbing Encryption Algorithm. *Mobile Networks and Applications, 16*(3), 304-336. doi:http://dx.doi.org/10.1007/s11036-011-0303-9

Cheong, S. N., Ling, H. C., & Teh, P. L. (2014). Secure Encrypted Steganography Graphical Password scheme for Near Field Communication smartphone access control system. *Expert Systems with Applications, 41*(7), 3561-3568. doi:10.1016/j.eswa.2013.10.060

Connie, T., Teoh, A., Goh, M., & Ngo, D. (2004). PalmHashing: a novel approach for dual-factor authentication. *Pattern Analysis and Applications, 7*(3), 255-268. doi:10.1007/s10044-004-0223-4

Dasgupta, D., Roy, A., & Nag, A. (2016). Toward the design of adaptive selection strategies for multi-factor authentication. *Computers & Security, 63*, 85-116. doi:10.1016/j.cose.2016.09.004

Gupta, P., & Dhar, J. (2016). Hash Based Multi-server Key Exchange Protocol Using Smart Card. *Wireless Personal Communications, 87*(1), 225-244. doi:10.1007/s11277-015-3040-8

He, D., Kumar, N., & Khan, M. (2013). Anonymous two-factor authentication for consumer roaming service in global mobility networks. *IEEE Transactions on Consumer Electronics, 59*(4), 811-817. doi:10.1109/TCE.2013.6689693

Hoang, T., Choi, D., & Nguyen, T. (2015). Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme. *International Journal of Information Security, 14*(6), 549-560. doi:10.1007/s10207-015-0273-1

Islam, S. K. H., & Khan, M. (2014). Cryptanalysis and Improvement of Authentication and Key Agreement Protocols for Telecare Medicine Information Systems. *Journal of Medical Systems, 38*(10), 1-16. doi:10.1007/s10916-014-0135-9

Jiang, Q., Ma, J., Wei, F., Tian, Y., Shen, J., & Yang, Y. (2016). An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks. *Journal of Network and Computer Applications*. doi:10.1016/j.jnca.2016.10.001

Juan, Q., & Xiao-Ling, T. (2014). Two-Factor User Authentication with Key Agreement Scheme Based on Elliptic Curve Cryptosystem. *Journal of Electrical & Computer Engineering*, 1-6. doi:10.1155/2014/423930

Karen D. Loch, a., Houston H. Carr, a., & Merrill E. Warkentin, a. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding. *Mis Quarterly*(2), 173. doi:10.2307/249574

Khan, M. K., Alghathbar, K., & Zhang, J. (2011). Privacy-preserving and tokenless chaotic revocable face authentication scheme. *Telecommunication Systems, 47*(3-4), 227-234. doi:http://dx.doi.org/10.1007/s11235-010-9314-2

Kiljan, S., Simoens, K., De Cock, D., Van Eekelen, M., & Vranken, H. (2016). A Survey of Authentication and Communications Security in Online Banking. *ACM Computing Surveys, 49*(4), 61:61-61:35. doi:10.1145/3002170

Kim, J., Lee, D., Jeon, W., Lee, Y., & Won, D. (2014). Security Analysis and Improvements of Two-Factor Mutual Authentication with Key Agreement in Wireless Sensor Networks. *Sensors, 14*(4), 6443-6462. doi:10.3390/s140406443

Ku, Y., Choi, O., Kim, K., Shon, T., Hong, M., Yeh, H., & Kim, J.-H. (2013). Two-factor authentication system based on extended OTP mechanism. *International Journal of Computer Mathematics, 90*(12), 2515-2529. doi:10.1080/00207160.2012.748901

Ku, Y., Choi, O., Kim, K., Shon, T., Hong, M., Yeh, H., & Kim, J. H. (2013). Two-factor authentication system based on extended OTP mechanism. *International Journal of Computer Mathematics, 90*(12), 2515-2529. doi:10.1080/00207160.2012.748901

Kumari, S., & Khan, M. K. (2014). Cryptanalysis and improvement of 'a robust smart-card-based remote user password authentication scheme'. *International Journal of Communication Systems, 27*(12), 3939-3955. doi:10.1002/dac.2590

Lat, J. A. S., Bondoc, R. X. R., & Atienza, K. C. V. (2013). SOUL System: secure online USB login system. *Information Management & Computer Security, 21*(2), 102-109. doi:http://dx.doi.org/10.1108/IMCS-08-2012-0042

Ma, B., Wang, Y., Li, C., Zhang, Z., & Huang, D. (2014). Secure multimodal biometric authentication with wavelet quantization based fingerprint watermarking. *Multimedia Tools and Applications, 72*(1), 637-666. doi:http://dx.doi.org/10.1007/s11042-013-1372-5

Ntantogian, C., Malliaros, S., & Xenakis, C. (2015). Gaithashing: A two-factor authentication scheme based on gait features. *Computers & Security, 52*, 17-32. doi:10.1016/j.cose.2015.03.009

Pang, Y. H., Andrew, T. B. J., & David, N. C. L. (2007). Two-factor cancelable biometrics authenticator. *Journal of Computer Science and Technology, 22*(1), 54-59. doi:10.1007/s11390-007-9006-x

Sarel, D., & Marmorstein, H. (2006). Addressing consumers' concerns about online security: A conceptual and empirical analysis of banks' actions. *Journal of Financial Services Marketing, 11*(2), 99-115. doi:http://dx.doi.org/10.1057/palgrave.fsm.4760025

Schneier, B. (2005). Two-factor authentication: Too little, too late. *Communications of the ACM, 48*(4), 136.

Shadish, W. R., Cook, T. D., & Campbell, D. T. (2001). *Experimental and quasi-experimental designs for generalized causal inference*: Boston : Houghton Mifflin, 2002.

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence‐informed management knowledge by means of systematic review. *British journal of management, 14*(3), 207-222.

Wang, D., Wang, N., Wang, P., & Qing, S. (2015). Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity. *Information Sciences, 321*, 162-178. doi:10.1016/j.ins.2015.03.070

Wei, J., Liu, W., & Hu, X. (2014). Cryptanalysis and Improvement of a Robust Smart Card Authentication Scheme for Multi-server Architecture. *Wireless Personal Communications, 77*(3), 2255-2269. doi:10.1007/s11277-014-1636-z

Yang, G. M., Wong, D. S., Wang, H. X., & Deng, X. T. (2008). Two-factor mutual authentication based on smart cards and passwords. *Journal of Computer and System Sciences, 74*(7), 1160-1172. doi:10.1016/j.jcss.2008.04.002

Yoo, C., Kang, B.-t., & Kim, H. K. (2015). Case study of the vulnerability of OTP implemented in internet banking systems of South Korea. *Multimedia Tools and Applications, 74*(10), 3289-3303. doi:http://dx.doi.org/10.1007/s11042-014-1888-3

Appendix A Studies included in this review

[1] Wang, F., Xu, Y. J., Zhang, H. W., Zhang, Y. J., & Zhu, L. H. (2016). 2FLIP: A Two-Factor Lightweight Privacy-Preserving Authentication Scheme for VANET. Ieee Transactions on Vehicular Technology, 65(2), 896-911. doi:10.1109/tvt.2015.2402166
[2] Jyh-Win, H., & Ting-Wei, H. (2007). A cost-effective add-on-value card-assisted firewall over Taiwan's NHI VPN framework. Medical Informatics & the Internet in Medicine, 32(2), 103-116. doi:10.1080/14639230601135497
[3] Hsieh, W. B., & Leu, J. S. (2014). A Robust User Authentication Scheme Using Dynamic Identity in Wireless Sensor Networks. Wireless Personal Communications, 77(2), 979-989. doi:10.1007/s11277-013-1547-4
[4] Ting, S. L., & Tsang, A. H. C. (2013). A two-factor authentication system using Radio Frequency Identification and watermarking technology. Computers in Industry, 64(3), 268-279. doi:10.1016/j.compind.2012.11.002
[5] Guo, M. H., Liaw, H. T., Deng, D. J., & Chao, H. C. (2011). An RFID secure authentication mechanism in WLAN. Computer Communications, 34(3), 236-240. doi:10.1016/j.comcom.2010.02.033
[6] Jiang, Q., Ma, J., Wei, F., Tian, Y., Shen, J., & Yang, Y. (2016). An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks. Journal of Network and Computer Applications. doi:10.1016/j.jnca.2016.10.001
[7] He, D. B., Kumar, N., Khan, M. K., & Lee, J. H. (2013). Anonymous Two-factor Authentication for Consumer Roaming Service in Global Mobility Networks. Ieee Transactions on Consumer Electronics, 59(4), 811-817.
[8] Jin, A. T. B., Ling, D. N. C., & Goh, A. (2004). Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recognition, 37(11), 2245-2255. doi:10.1016/j.patcog.2004.04.011
[9] Khan, M. K., Zhang, J. S., & Wang, X. M. (2008). Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices. Chaos Solitons & Fractals, 35(3), 519-524. doi:10.1016/j.chaos.2006.05.061
[10] Go, W., Lee, K., & Kwak, J. (2014). Construction of a secure two-factor user authentication system using fingerprint information and password. Journal of Intelligent Manufacturing, 25(2), 217-230. doi:10.1007/s10845-012-0669-y
[11] Wei, J. H., Liu, W. F., & Hu, X. X. (2014). Cryptanalysis and Improvement of a Robust Smart Card Authentication Scheme for Multi-server Architecture. Wireless Personal Communications, 77(3), 2255-2269. doi:10.1007/s11277-014-1636-z
[12] Kumari, S., & Khan, M. K. (2014). Cryptanalysis and improvement of 'a robust smart-card-based remote user password authentication scheme'. International Journal of Communication Systems, 27(12), 3939-3955. doi:10.1002/dac.2590
[13] Chaudhry, S. A., Naqvi, H., Shon, T., Sher, M., & Farash, M. S. (2015). Cryptanalysis and Improvement of an Improved Two Factor Authentication Protocol for Telecare Medical Information Systems. Journal of Medical Systems, 39(6). doi:10.1007/s10916-015-0244-0
[14] Islam, S. K. H., & Khan, M. K. (2014). Cryptanalysis and Improvement of Authentication and Key Agreement Protocols for Telecare Medicine Information Systems. Journal of Medical Systems, 38(10). doi:10.1007/s10916-014-0135-9
[15] Xie, Q., Dong, N., Wong, D. S., & Hu, B. (2016). Cryptanalysis and security enhancement of a robust two-factor authentication and key agreement protocol. International Journal of Communication Systems, 29(3), 478-487. doi:10.1002/dac.2858
[16] Jiang, Q., Ma, J. F., & Tian, Y. L. (2015). Cryptanalysis of smart-card-based password authenticated key agreement protocol for session initiation protocol of Zhang et al. International Journal of Communication Systems, 28(7), 1340-1351. doi:10.1002/dac.2767
[17] Chang, I. P., Lee, T. F., Lin, T. H., & Liu, C. M. (2015). Enhanced Two-Factor Authentication and Key Agreement Using Dynamic Identities in Wireless Sensor Networks. Sensors, 15(12), 29841-29854. doi:10.3390/s151229767
[18]Hoang, T., Choi, D., & Nguyen, T. (2015). Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme. International Journal of Information Security, 14(6), 549-560. doi:10.1007/s10207-015-0273-1

[19] Ntantogian, C., Malliaros, S., & Xenakis, C. (2015). Gaithashing: A two-factor authentication scheme based on gait features. Computers & Security, 52, 17.
[20] Gupta, P., & Dhar, J. (2016). Hash Based Multi-server Key Exchange Protocol Using Smart Card. Wireless Personal Communications, 87(1), 225-244. doi:10.1007/s11277-015-3040-8
[21] Cao, T. J., & Zhai, J. X. (2013). Improved Dynamic ID-based Authentication Scheme for Telecare Medical Information Systems. Journal of Medical Systems, 37(2). doi:10.1007/s10916-012-9912-5
[22] Arshad, H., Teymoori, V., Nikooghadam, M., & Abbassi, H. (2015). On the Security of a Two-Factor Authentication and Key Agreement Scheme for Telecare Medicine Information Systems. Journal of Medical Systems, 39(8). doi:10.1007/s10916-015-0259-6
[23] Connie, T., Teoh, A., Goh, M., & Ngo, D. (2004). PalmHashing: a novel approach for dual-factor authentication. Pattern Analysis and Applications, 7(3), 255-268. doi:10.1007/s10044-004-0223-4
[24] Wang, D., Wang, N., Wang, P., & Qing, S. (2015). Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity. Information Sciences, 321, 162-178. doi:10.1016/j.ins.2015.03.070
[25] Bhargav-Spantzel, A., Squicciarini, A. C., Modi, S., Young, M., Bertino, E., & Elliott, S. J. (2007). Privacy preserving multi-factor authentication with biometrics. Journal of Computer Security, 15(5), 529-560.
[26] Bhargav-Spantzel, A., Squicciarini, A. C., Modi, S., Young, M., Bertino, E., & Elliott, S. J. (2007). Privacy preserving multi-factor authentication with biometrics. Journal of Computer Security, 15(5), 529-560.
[27] Xie, Q., Hu, B., Tan, X., Bao, M. J., & Yu, X. Y. (2014). Robust Anonymous Two-Factor Authentication Scheme for Roaming Service in Global Mobility Network. Wireless Personal Communications, 74(2), 601-614. doi:10.1007/s11277-013-1309-3
[28] Khan, S. H., Akbar, M. A., Shahzad, F., Farooq, M., & Khan, Z. (2015). Secure biometric template generation for multi-factor authentication. Pattern Recognition, 48(2), 458-472. doi:10.1016/j.patcog.2014.08.024
[29] Cheong, S. N., Ling, H. C., & Teh, P. L. (2014). Secure Encrypted Steganography Graphical Password scheme for Near Field Communication smartphone access control system. Expert Systems with Applications, 41(7), 3561-3568. doi:10.1016/j.eswa.2013.10.060
[30] Ma, B., Wang, Y., Li, C., Zhang, Z., & Huang, D. (2014). Secure multimodal biometric authentication with wavelet quantization based fingerprint watermarking. Multimedia Tools and Applications, 72(1), 637-666. doi:http://dx.doi.org/10.1007/s11042-013-1372-5
[31] Arshad, H., & Nikooghadam, M. (2015). Security analysis and improvement of two authentication and key agreement schemes for session initiation protocol. Journal of Supercomputing, 71(8), 3163-3180. doi:10.1007/s11227-015-1434-8
[32] Kim, J., Lee, D., Jeon, W., Lee, Y., & Won, D. (2014). Security Analysis and Improvements of Two-Factor Mutual Authentication with Key Agreement in Wireless Sensor Networks. Sensors, 14(4), 6443-6462. doi:10.3390/s140406443
[33] Cheng, F. (2011). Security Attack Safe Mobile and Cloud-based One-time Password Tokens Using Rubbing Encryption Algorithm. Mobile Networks & Applications, 16(3), 304-336. doi:10.1007/s11036-011-0303-9
[34] Joshua Arvin, S. L., Rod Xavier, R. B., & Atienza, K. C. V. (2013). SOUL System: secure online USB login system. Information Management & Computer Security, 21(2), 102-109. doi:http://dx.doi.org/10.1108/IMCS-08-2012-0042
[35] Ku, Y., Choi, O., Kim, K., Shon, T., Hong, M., Yeh, H., & Kim, J. H. (2013). Two-factor authentication system based on extended OTP mechanism. International Journal of Computer Mathematics, 90(12), 2515-2529. doi:10.1080/00207160.2012.748901
[36] Pang, Y.-h., J, A. T., & L, D. N. (2007). Two-Factor Cancelable Biometrics Authenticator. Journal of Computer Science and Technology, 22(1), 54-59. doi:http://dx.doi.org/10.1007/s11390-007-9006-x
[37] Yang, G. M., Wong, D. S., Wang, H. X., & Deng, X. T. (2008). Two-factor mutual authentication based on smart cards and passwords. Journal of Computer and System Sciences, 74(7), 1160-1172. doi:10.1016/j.jcss.2008.04.002
[38] Juan, Q., & Xiao-Ling, T. (2014). Two-Factor User Authentication with Key Agreement Scheme Based on Elliptic Curve Cryptosystem. Journal of Electrical & Computer Engineering, 1-6. doi:10.1155/2014/423930