Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

Using a systematic framework to critically analyze proposed smart card based two factor authentication schemes

Khalid Hussain[a], NZ Jhanjhi[b,*], Hafiz Mati-ur-Rahman[c], Jawad Hussain[d], Muhammad Hasan Islam[e]

[a] University of Lahore, Islamabad Campus, Pakistan
[b] School of Computing and IT (SoCIT), Lakeside Campus, Taylor's University, Subang Jaya, Selangor, Malaysia
[c] Centre for Advanced Studies in Engineering (CASE), Islamabad, Pakistan
[d] University of Engineering and Technology Taxila, Pakistan
[e] Youth University, Islamabad, Pakistan

ARTICLE INFO

Article history:
Received 3 November 2018
Revised 21 January 2019
Accepted 30 January 2019
Available online xxxx

Keywords:
Two factor authentication
Smart cards
Systematic framework
Protocol
Scheme
Rating
Multi-factor authentication

ABSTRACT

The importance of smart card based two factor authentication can be gauged by the fact that many schemes have been proposed so far yet none of them used a systematic framework to critically analyze themselves to prove them practical and use worthy. This research however accomplishes exactly this by showing how using a criteria set can aid in highlighting the underlying hidden weaknesses in the design of the proposed schemes and what can be done to improve them by incorporating security features from the initial development stages of the protocols. This would also ensure only meaningful contribution in developing stronger schemes. Our research also lays the foundation stone by assessing the latest scheme proposed by Xie et al. and suggesting improvements in it. And finally, a novel scheme rating mechanism has been introduced to rate schemes thus helping in determining the actual goodness of the schemes and facilitating top managements of corporate sectors to make informed decisions.

1. Introduction

Authentication using a password is extensively used as an access control mechanism in order to limit access to resources to authorized users only. Authorized users present the password registered against their user id, to the authentication server which stores a password verifier table. Password is verified and the users are given access. This mechanism can be seen in the schemes of Abdalla et al. (2015) and Wu (1998). This mechanism is very popular due to being very cost effective and scalable Bonneau et al. (2012). However, if this password verifier table, stored in the sever, is leaked, the whole system collapses. One of the many examples of such incidents are the breach of all user accounts (3 Billion) of Yahoo (http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html, 2019) in August 2013. Others include Gmail (4.9 Million) (https://www.scmagazine.com/report-dark-web-vendor-selling-millions-of-gmail-and-yahoo-accounts/article/645174/, 2019), Anthem (80 Million) (https://duo.com/blog/four-years-later-anthem-breached-again-hackers-stole-employee-credentials, 2019) to name a few. The system will also collapse if the user accidently shares the password with an attacker. This can be achieved using social engineering attacks, phishing to name a few methods. Users may also write down the password on a piece of paper if the system requires the password to be very complex and long, even worse if issued by the system itself because humans have inherently a weak memory. One would argue that may be passwords stored in hashed format may help but as Gosney (2012) showed that a rig of 25 GPU's can check up to 350 billion passwords per second in an offline dictionary attack against the hash functions. To counter the password leakage issue, different mechanisms have been proposed which include user related information and password being spread over multiple servers and the compromise of multiple servers is required to complete the hack (Camenisch et al., 2015) but they fail to deal with user end password leakages due to social engineering and phishing attacks as mentioned above. Leakage resilient password systems (Weinshall, 2006) have been put forward which

[*] Corresponding author.
E-mail address: noorzaman.jhanjhi@taylors.edu.my (NZ Jhanjhi).

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2019.01.015
1319-1578/© 2019 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University.

require an indirect keying in of the password by the user which is very unfriendly.

The introduction of smart card as the second factor of authentication along with the first factor being a password was first put forth twenty-seven years ago (Chang and Wu, 1991) and has been widely used in applications requiring enhanced security like online banking, online trading etc. In this setting, a user registers himself to the server with user selected username and password. A smart card is issued by the server for the user in a secure manner. The smart card contains some security parameters. Now the user will use both his password and smart card for further authentication with the server. A generic smart card based two factor authentication is shown in the block (flow) diagram Fig. 1.

Many smart card based password authentication schemes were proposed one after the other e.g. Xu et al. (2009), Sood et al. (2010), Chen et al. (2012), Xie et al. (2016). The authors would propose a scheme which boasts to support certain useful security properties but shortly after the schemes are proven to be insecure or vulnerable to attacks. So these schemes are then "improved" and put forth. Yet, the improved schemes are again proven to be insecure or vulnerable and are further improved and this cycle would go on and on.

Rest of the paper is organized as following. Section 2 discusses about the motivation for this research. Section 3 details our contribution and finally Section 4 details the conclusion, recommendation and future work.

2. Motivation

While so many different schemes were being proposed one after another and the same schemes were being "improved" and then broken again and improved again and this cycle continued, the logical and natural need arose of which was to have the proposed scheme fulfill a certain criteria set of requirements. Hence, different set of objectives, or design goals or criteria were proposed most notably some of which were Yang et al. (2008), Wang et al. (2011), Liao et al. (2006), Tsai et al. (2006). Madhusudhan and Mittal (2012) criteria set was a good refinement of the above mentioned criteria sets which showed that the previously proposed two factor authentication schemes are not supreme and they have their positive and negative aspects.

Wang et al. (2015) explores the Madhusudhan et al. criteria set and the interconnections between criteria points and highlights that while designing anonymous two factor authentication schemes, there are some intrinsic clashes and inevitable compromises that have to be taken care of leading to which he concludes that it is not possible to build an ultimate or ideal two factor authentication protocol. Wang et al. (2015) has tried to highlight that if the inevitable compromises are made (but they should be acceptable also) and inbuilt clashes are resolved in the criteria proposed for two factor authentication schemes, only then it would be possible to understand how such schemes can be built which will support important features like being secure, practical and taking care of user privacy. Also, Wang et al. (2015) concludes that "security-usability" tension as presented in his paper suggests that there does not exist a smart card based password authentication protocol with local password update which is secure as well thus answering the open question left by Huang.

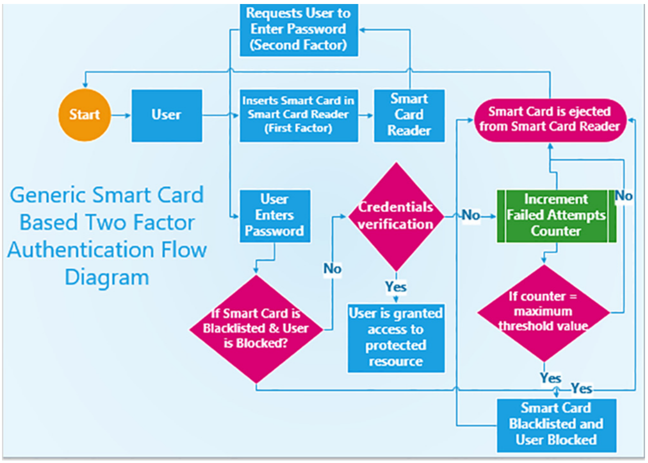
Requests User to Enter Password (Second Factor)
Start
User
Inserts Smart Card in Smart Card Reader (First Factor)
Smart Card Reader
Smart Card is ejected from Smart Card Reader
Generic Smart Card Based Two Factor Authentication Flow Diagram
User Enters Password
Credentials verification
No
Increment Failed Attempts Counter
No
No
Yes
If Smart Card is Blacklisted & User is Blocked?
User is granted access to protected resource
If counter = maximum threshold value
Yes
Yes
Smart Card Blacklisted and User Blocked

Fig. 1. Generic Smart Card Based Two Factor Authentication Block Diagram.

Wang et al. (2015) mentions that there are two other factors besides evaluation criteria that are going to help in designing better smart card based anonymous two factor authentication schemes and they are system architecture and adversarial model. Among tens of hundreds of schemes proposed only a handful of schemes some which are Yang et al. (2008), Wang (2012) and Wang et al. (2014) outline the above mentioned three factors. Wang et al. (2015) also introduces a novel solution for secure password change in smart card based password two factor authentication schemes known as "Fuzzy Verifier". Its effectiveness has also been proven by Wang and Wang (2016) as well on his website by performing a series of tests on password database.

Wang and Wang (2016) also proposed a set of 12 criteria points which should be satisfied by a two factor authentication scheme based on earlier proposed criteria sets namely Wang et al. (2015), Yang et al. (2008) and Madhusudhan et al., some earlier obtained conclusions Wang et al. (2015), Wang and Wang (2014), Wang et al. (2016) and criteria refinement methodology Bonneau et al. In order to have a better understanding of how the criteria sets evolved over the years, we have compiled a table comparing different criteria sets with the one used in this research. This will also show the strength and comprehensive nature of the criteria set used for benchmarking schemes in this research. The table is shown below Table 1.

Wang and Wang (2016) along with proposing comprehensive criteria also proposed a harshest and realistic adversary model as well as takes care of the system architecture. Wang and Wang (2016) also proposes a two factor authentication scheme that satisfies the strict 12 criteria framework.

Since now a comprehensive criteria set is at hand along with schemes that have not been checked against the proposed criteria, it is imperative to use the proposed framework to critically analyze previously unchecked schemes for possible weaknesses, practicality and usability.

Also, there is no scheme rating mechanism proposed so far

3. Our contribution

In this research, we have done the following three contributions

Firstly, we have critically analyzed Xie et al. (2017) scheme in detail using Wang and Wang (2016) 12-point criterion set and dug out weaknesses and suggested improvements.

In a similar fashion, we critically analyzed some previously proposed schemes

Finally, we proposed a scheme rating mechanism

3.1. Review of Xie et al. (2017) scheme

Before critically analyzing Xie's et al. scheme, it is important to first understand his scheme. It is essentially a dynamic ID based or anonymous two factor authentication key exchange protocol. By Dynamic ID based or anonymous, it means that the identity of

Please cite this article as: K. Hussain, N. Jhanjhi, H. Mati-ur-Rahman et al., Using a systematic framework to critically analyze proposed smart card based two factor authentication schemes, Journal of King Saud University – Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2019.01.015

Table 1
Major criteria sets proposed over the years.

Criteria	Madhusudhan and Mittal (2012)	Wang et al. (2011)	Yang et al. (2008)	Tsai et al. (2006)	Liao et al. (2006)
No Password Verifier Table	Yes	Yes	Yes	Yes	No
Password Friendly					
i. Memorable	i. Yes	i. Yes	i. Yes	i. Yes	i. Yes
ii. Chosen Freely	ii. Yes	ii. Yes	ii. Yes	ii. Yes	ii. Yes
iii. Changed Locally by the user	iii. No (Completely Missing)	iii. No	iii. Yes	iii. No	iii. Yes
No Password Exposure	Yes	Yes	Yes	Yes	Yes
No Smart Card Loss Attack	Yes	Yes	No	Yes	Yes
Resistance to Known Attacks					
i. Offline PWD Guessing	i. Yes	i. Yes	i. No	i. Yes	i. Yes
ii. Replay	ii. Yes	ii. Yes	ii. No	ii. Yes	ii. Yes
iii. Parallel Session	iii. Yes	iii. No	iii. No	iii. Yes	iii. No
iv. De-Synchronization	iv. No	iv. No	iv. No	iv. No	iv. No
v. Stolen Verifier	v. Yes	v. Yes	v. Yes	v. Yes	v. Yes
vi. Impersonation	vi. Yes	vi. Yes	vi. No	vi. Yes	vi. Yes
vii. Unknown Key Share	vii. No	vii. No	vii. No	vii. No	vii. No
viii. Know Key	viii. No	viii. Yes	viii. No	viii. No	viii. No
Sound Repairability	No	Yes	No	No	No
Provision of Key Agreement	Yes	Yes	No	Yes	No
No Clock Synchronization	No	Yes	No	No	No
Timely Typo Detection	Yes	No	No	Yes	No
Mutual Authentication	Yes	No	Yes	Yes	Yes
User Anonymity	Yes	No	No	No	No
Forward Secrecy	Yes	No	No	Yes	No

the user is not the actual identity rather a pseudo identity which the user picks himself or herself and sends it to the server. It may or may not change in every session but it will not be the user's real identity.

Now as Xie et al. mentions in his paper some specifications for his scheme which are as below

- Scheme is based on elliptic curve cryptosystem (ECC)
- p is a large prime number
- E_p is a p-order elliptic curve group defined over $GF(q)$ where q is a prime or in binary space 2^n
- G is the generator of the group E_p
- E_k and D_k is symmetric encryption and decryption under key k of a remote server S
- x is a long term secret key of S
- SC stands for Smart Card
- PW represents the user's password
- SK is Session Key
- $h1()$is a cryptographic hash function which maps to p-order cyclic group of integers Z_p
- $h2()$ and $h2'()$are cryptographic hash functions that map to 256 bit strings

There are four Phases of Xie's et al. Scheme which are user registration, login and authentication, password change and smart card revocation. The phases are briefly explained below

In the first step of user registration, a user U can randomly choose a pseudo identity ID_u and then send to the server S using a secure channel.

Then the Server S randomly picks its pseudo identity namely ID_s a smart card identifier namely CI, a randomly selected nonce N_0which is for the particular user U. Then the server computes the ID by concatenating ID_u, ID_s and CI

$$ID = ID_u||ID_s||CI$$

Then DID is computed by first concatenating ID and N_0then encrypting the result with server's S long term secret key x as shown below as well

$$DID = E_x(ID||N_0)$$

Then V_0 is calculated by concatenating ID and long term secret key x of server and then hashing the result to get a big number V_0 in Z_p domain as shown below

$$V_0 = h_1(ID||x)$$

Then the server S writes the DID and V_0 in Smart Card and now the Smart Card is ready to be sent to user via a secure channel. The server S stores the concatenated id ID, Card Identifier CI and a counter namely $CTR_s vr$ in its registration table. The counter is used by the server to track the failed authentication attempts by the user with his id ID_u and the particular card identifier CI selected by the server for this user. The value of this counter is set to Zero initially. The parameter n is the threshold value used to detect online dictionary attacks. $CTR_s vr$and CTR_SC should always be less than the value n where CTR_SC is the counter parameter in smart card used to count the failed attempts by the server to authenticate itself to the user.

Next, when the smart card is received by the user, he will insert the smart card in the smart card reader and will choose a password PW. The parameter V is calculated in the following way

$$V = Vo \oplus h1(PW)$$

The XOR done is bit wise XOR. The cryptographic hash function $h1()$ as stated earlier will output a large number in Z_p domain. This calculated V replaces the already stored V_0in the smart card. At this point CTR_SC is also stored in Smart Card and now the updated parameters in the smart card are V, DID, CTR_SC and threshold parameter n. Now the user is ready to do login and authentication attempts.

In the login and authentication phase, the user U inserts the smart card in to the smart card reader and enters the pseudo identity ID_u and PW. First the value of CTR_SC is checked which should be less then n in order for the protocol to proceed. If yes, the smart card randomly selects a nonce r in Z_p domain and computes

$$e = r * G$$

$$V_0 = V \oplus h_1(PW)$$

Which will equal to $V = h_1(ID||x)$ because if we put the value of V in the above equation it will become

$$V_0 = V_0 \oplus h_1(PW) \oplus h_1(PW)$$

Now replacing $V_0$with $h_1(ID||x)$ since its stored in smart card

$$V_0 = h_1(ID||x)$$

Also computed is

$$V_1 = e + h_1(V_0||ID_u||T_1) * G$$

where T_1 is the current timestamp

In the calculation of e we note that the generator of the elliptic group G is multiplied with random value r. This is basically adding the generator G, r times which essentially shifting the point G on elliptic curve, r times on the elliptic curve. In elliptic curve cryptography, this is essentially this is known as ECC discrete logarithm or ECC DH computation because finding e by guessing r is impossible.

Now Smart Card sends V_1, DID and T_1 to the server, otherwise the protocol aborts (when the CTR_SC less then n check fails)

When the server receives the parameters, it checks the freshness of timestamp T_1. If it is within the threshold (which is predefined) only then the following steps are done which are

1. Decryption of DID in order to extract ID
2. This would revealID_u, ID_s, CI (which are checked for validity) and N_0. If they are found to be invalid, S terminates the protocol else it continues as below
3. Then $CTR_s\,vr$value is checked which should be less than n which if not less than n, the protocol is terminated otherwise the protocol continues as below

Now e is calculated at server end in the following way

$$e = V_1 - h_1(V_0||ID_u||T_1) * G$$

Putting the value of V_1 in the above equation will give us

$$e = e + h_1(V_0||ID_u||T_1) * G - h_1(V_0||ID_u||T_1) * G$$

$e = e$ (so e is being calculated correctly)

Once e is obtained it is used to calculate$c$

$$c = u * e$$

where u is randomly picked nonce. Then d is calculated using u as below

$$d = u * G$$

Then NID, V_2 and V_3 are calculated as below

$$NID = E_x(ID||N_1)$$

$$V_2 = h_2(c) \oplus NID$$

$$V_3 = h_2(NID||c||T_2)$$

Now Server sends V_2, V_3, d and T_2 (current timestamp) to smart card. In case, the server receives another request message (V_1', DID, T_1') with the same DID at T_1' but didn't receive V_4 which had to be related to (V_1, DID,T_1), the Server increments the counter $CTR_s\,vr$ by 1 and the protocol aborts.

Now when the smart card receives the parameters V_2, V_3, d and T_2, the first of the checks which is performed is whether T_2 is within the pre-defined threshold or not. If it is within the threshold, then the protocol continues otherwise the protocol aborts. The protocol continues by calculating

$$c = r * d$$

Since $d = u * G$ so c becomes

$$c = r * u * G$$

$$NID = V_2 \oplus h_2(c)$$

Now here it is checked whether $V_3 = h_2(NID||c||T_2)$ or not. This will authenticate the server S. If the check is true, the smart card calculates

$$V_4 = h_2(V_1||c)$$

$$SK = h_2(c||d||e)$$

Stored DID in smart card is replaced by NID

Send V_4 to server

If the check of V_3 fails, CTR_SC is incremented by 1 and the protocol is terminated.

When the server receives V_4, it calculates V_4 which should be equal to the received V_4 as it will authenticate the user. V_4 is calculated as below

$$V_4 = h_2(V_1||c)$$

Then SK is calculated as below

$$SK = h_2(c||d||e)$$

If the check of V_4 fails, the $CTR_s\,vr$ is incremented by 1 and the protocol aborts.

For change of password, the user has to enter the current password PW and has to go through the complete authentication phase with the server. Once authenticated, then the user enters the new password PW^*. The Smart Card will compute the following

$$V^* = V \oplus h_1(PW) \oplus h_1(PW^*)$$

It will equal to

$$V^* = V_0 \oplus h_1(PW) \oplus h_1(PW) \oplus h_1(PW^*)$$

Since $V_0 = h_1(||x)$so

$$V^* = h_1(ID||x) \oplus h_1(PW^*)$$

Then V is replaced by V^* in the smart card.

In case of smart card revocation, which may be required if the user's smart card is stolen or lost, the user can request a new smart card to server who will issue a new smart card after verifying the user's current pseudo identityID_u. The server generates the new smart card identifier CI', a nonce N_0, computing ID, $DID$and V_0as below

$$ID = ID_u||ID_s||CI'$$

$$DID = E_x(ID||N_0)$$

$$V_0 = h_1(ID||x)$$

DID and $V_0$are stored in smart card and then the smart card is sent to user via a secure channel. The server stores new ID, CI' and $CTR_s\,vr$ in registration table (so we can see that smart card revocation process is same as a normal registration phase). $CTR_s\,vr$ is set to zero.

3.2. Critical analysis of Xie et al. (2017) scheme

Below is the critical analysis of Xie's et al. scheme in the light of Wang and Wang (2016) criteria set.

3.2.1. No password verifier table

In Xie's et al. scheme, it is noted that when the user enters his password for logging in during authentication phase, the parameters which are calculated in the smart card are $V_0$and V_1 and 'e'. $V_0$is computed by XORing V and hash of user password which results in the hash value of concatenated ID and server's long term secret key 'x'. Note that the effect of hash of user password is removed because V is computed by XORing concatenated ID and server's long term key 'x' with hash of user registered or current password. V_1 is computed by XORing e with hash of concatenated parameters namely V_0 (just computed), user *ID* and current timestamp multiplied with *G* which is the generator of the *p*-order elliptic curve group Ep. This V_1, along with encrypted concatenated *ID* and N_0 (chosen by server for this user during registration phase) with server's long time secret key '*x*' along with current timestamp are sent by Smart Card to server for verification. Concatenated id*ID* is actually concatenation string of user Id ID_u, server Id $ID_s$and smart card identifier *CI*. Now we can see that the user does not send a password for his verification neither a derived value of user password so we conclude that Xie's et al. scheme does meet Wang's et al. first criterion.

3.2.2. Password Friendly

Xie's et al. scheme does not furnish password to the user which means that the user can choose the password of his own liking and which will be memorable for him. Also after the critical analysis of Xie's et al. scheme, it is noted that his scheme does not support local password change rather it involves the interaction with server. Also, it asks the user to enter the new password twice. The user first has to authenticate him or herself with the server using a normal authentication and logging in procedure and then the user can initiate the password change. The author has cited the reasons for interacting with server and he says that

In order to update the password locally without the interaction with server, a password authenticator has to be stored in the smart card which if leaked can lead the attacker to launch an offline password guessing attack.

A user may accidently enter an unintended password during the password change phase and update the smart card with an unknown password thus making the smart card unusable for future use

First we tackle the second point. The said possibility can simply be taken care of if the scheme supporting local password update, asks the user to enter the password twice.

Now we come to the first point. Wang and Wang (2016) and Wang et al. (2014) has showed that offline password guessing attack can be taken care of if a scheme supports local password update by using a parameter called "fuzzy verifier" effectiveness of which has been shown by Wang and Wang (2016) in his paper. So we show here that Xie's et al. scheme does not meet the criterion of local password update. The reason cited by the author does not stand valid if fuzzy verifier is used as shown by Wang and Wang (2016) in his paper. Xie's et al. scheme can be thus improved after the inclusion of fuzzy verifier. Also, the criteria framework shows its effectiveness by not only highlighting weaknesses in the proposed scheme but also suggests ways to improve the proposed scheme.

3.2.3. No password Exposure

In Xie's et al. scheme it was found that even if the administrator of the server has complete administrator rights, still he or she cannot derive the passwords because user passwords are not sent rather hashed value of concatenated *ID* and server's long term secret key and other derived parameters are sent to the server for authentication. Consequently, at the server side, parameters are calculated which if matched for example parameter *e*, ensures the correctness of password upon which further new parameters are calculated on the server side based upon *e*. So Xie's et al. scheme does meet the criterion of no password exposure.

3.2.4. No smart card Loss attack

In Xie's et al. scheme, it is noted that his scheme is not prone to smart card loss attack. Because let's assume that

The owner of the smart card has lost his or her smart card somewhere or the smart card has been stolen.

The smart card has been compromised and not yet revoked by user from backend

The adversary has been able to extract the stored information from the smart card and has obtained *DID* and *V*.

The adversary has recorded all the sent and received messages in the protocol execution

The user has been social engineered in to revealing his user id ID_u.

Now for the following equation to satisfy the adversary has to guess the password

$$V_0 = V \oplus h_1(PW)$$

So the adversary launches and offline password guessing attack. Note here that the adversary also has to calculate the parameter *e* which is computed once $V_0$is computed. The equation for parameter e is

$$e = V_1 - (h_1(V_0||\mathrm{ID}_u||T_1))G$$

Now when *e* is calculated, the attacker still has to calculate *c* and *d*. If the adversary is able to break Diffie-Hellman and calculate *c* and *d* after which the attacker can calculate V_3. But, breaking Diffie-Hellman is not possible so the scheme is not prone to Smart Card Loss Attack and offline password guessing attack. Another Scenario in the smart card loss attack could be that the adversary tries to use a revoked smart card. In that case, the identity of the revoked smart card has already been replaced by the identity of the updated smart card issued to user and when the revoked smart card is attempted to be used for authentication, it would be detected during authentication phase and thus the adversary would not be able to successfully pass through the authentication phase. So Xie's et al. scheme is not prone to Smart Card Loss Attack and thus it does meet the criterion.

3.2.5. Resistance to known attacks

As shown in the previous section, Xie's et al. scheme is not prone to offline password guessing attack due to intractability of computation of Diffie-Hellman problem.

The scheme is using timestamps (T_1 and T_2) in order to ward of replay attacks. Also nonces (r,u) are being used as well. Timestamps would be helpful in checking the freshness of the received messages as any delayed messages which may be due to the adversary replaying the messages will be discarded when not received within a pre-defined threshold to time. Also, in case the adversary is strong enough to replay the messages within the stipulated time period, he would still not be able to compute the parameters *c*,*d*,*e* due to not being able to know the nonces used which are *r* and *u* of which *r* is randomly picked over a large Z_p and *u* being randomly chosen and also due to impossibility of solving the Diffie-Hellman problem.

Since the basic premise of any form of parallel session attack is that the adversary replays the captured messages from one session to other parallel sessions, none of the form of parallel session attack would be successful in Xie's et al. scheme and the reason is even if the intruder replays the parameters of one session e.g. V_1, *DID*, T_1, the calculation of parameters based on nonces randomly selected by both client and server would not match with the what is calculated on the basis of parameters replayed by the attacker which were randomly chosen earlier by client and server.

Xie's et al. scheme does not maintain any pseudo identity of the user from the current protocol run to be used in the following protocol run rather the user after choosing its pseudo identity sends it to the server via a secure channel and the server calculates a concatenated *ID* based on the concatenation of its own id i.e.ID_s, user id sent by user to server which isID_u and N_0chosen by the server for this particular user. This is then encrypted with the sever long term secret key x to calculate DID which is then stored in Smart Card and sent to user and which will be used for the future protocol runs until the user decides to change his identity for any reason. So this scheme is not prone to de-synchronization attack.

Since Xie's et al. scheme is supports the feature of no password table, the risk of this attack is mitigated.

As mentioned earlier in replay attack, due to the intractability of DH problem, even if the attacker replays the captured messages, he or she still would not be successful in the impersonation attack.

Since in Xie's et al. scheme the client and server authenticate each other i.e. the scheme supports mutual authentication as shown below in the upcoming section, so unknown key share attack is not possible on Xie's et al. scheme.

Xie's et al. scheme basically depends on the nonces (r, u) that are chosen independently for each and every session and does not have any link to past or future sessions. These nonces are then used to calculate $c, d,$ and e which are then used to calculate sessions keys. Also the nonces are not transmitted during the protocol run so the cannot be recovered from the captured messages trivially. So the adversary cannot calculate the session keys and consequently the key cannot be breached which is why the scheme is not prone to Known Key Attack. So Xie's et al. scheme is not prone to known attacks and thus it does meet the criterion.

3.2.6. Sound Repairability

In the Xie's et al. scheme it is found that the user would not have to change the identity in case the smart card is lost because if that happens, the user would just request a new smart card from the server and the server after checking the ID of the user ID_u would issue him or her the new smart card. The server will generate a new Smart Card identifier which will lead to new concatenated ID (not the user ID as it remains the same) because of the new Card identifier being used in the concatenated id ID calculation. All the remaining calculation would remain the same. The process of issuing new smart card is exactly the same as when the user registers for the very first time. So Xie's et al. scheme does meet the criterion of sound repairability.

3.2.7. Provision of key agreement

After the critical analysis of the scheme, it is found that a mutual session key is agree upon between the server and the client in order to secure the communication. So Xie's et al. scheme does meet the criterion of provision of key agreement.

3.2.8. No clock synchronization

After the critical analysis of Xie's et al. scheme it is found that timestamps are being used to check freshness of the messages. If a message does not arrive within a defined threshold, it is discarded and the protocol is terminated. This is done to ward of replay attacks. However, an important point to note here is that what if a legitimate message arrives late due to non-synchronicity between clocks for smart cards and the server, still the legitimate user messages will be discarded and protocol will be terminated and the legitimate user would not be able to login. This shows that clock synchronicity is a must in order for the scheme to work. This is clearly against the criterion proposed which requires the scheme to be free from the clock synchronicity requirement. However, there is big catch here. While the scheme indeed fails to meet the proposed criterion, it can be made to work even if we remove the timestamp from the scheme i.e. replay attacks can still be warded off without using timestamps. It is because the scheme makes intelligent and extensive use of nonces. Even if the attacker intercepts the messages and replays them, he would still have to calculate the nonces which is not possible. Thus we show here that the scheme does not meet the criterion of no clock synchronization. It is recommended that the scheme be modified to make it satisfy the criterion thus improving the scheme, making it computationally and cost effective at the same time. This can be achieved by removing the timestamp check from the protocol. This also goes to show how robust the proposed criteria set is and how effective is it in improving the proposed schemes.

3.2.9. Timely typo detection

In Xie's et al. scheme, it is noted that the scheme does not support timely typo detection rather the incorrect credentials are sent to the server and it is until the last step of session key computation that the user is actually authenticated or not and thus the session key is either calculated or not. So, we can conclude that Xie's et al. scheme does not verify user credentials within the smart card and so it does not meet the criterion of Timely Typo Detection. It is recommended that the scheme author should utilize the fuzzy verifier solution to meet this criterion.

3.2.10. Mutual authentication

After the critical analysis of Xie's et al. scheme, it is noted that the scheme does authenticate bother server and the client or user. The calculation of parameters V_3 and V_4 are used for this purpose. V_3 is used for server authentication and V_4 is used for client authentication. So we conclude that the proposed scheme does meet the proposed criterion of mutual authentication.

3.2.11. User anonymity

After the critical analysis of Xie's et al. scheme, it is found out that for the adversary to find out the user identity which can be either ID_u or DID or both. For ID_u or DID, the adversary needs to know the password of the user. Along with the password of the user, the adversary has to find out the long term secret key x. Even if we assume that the adversary finds out the two secret parameters, yet the adversary has to solve the Diffie – Hellman problem to find the value of c to get to the identities. It is to be noted that each session is different from the other session due to the calculation of the session key SK based on the random nonces like N_1, r and u. So apart from user anonymity, the scheme also provides user intractability. So we conclude that the proposed scheme does meet the criterion of user anonymity.

3.2.12. Forward secrecy

As mentioned in the previous criterion, temporary session keys are being used for encryption of messages in each session. These session keys are being calculated using randomized nonces r and u and Diffie-Hellman technique. Even if the server's long term secret key is leaked, it would be extremely difficult for the adversary to solve Diffie-Hellman problem. Even if we assume that the adversary solves the Diffie-Hellman problem, then that would enable him to decrypt only this session keys, and for the next session, the adversary has to make the effort again from scratch to solve Diffie-Hellman problem for the next session so we conclude that the proposed scheme does provide Forward Secrecy.

3.3. Critical analysis of other previously proposed schemes

Below are the summarized results after critical analysis of other schemes using Wang's criteria set for the sake of brevity Table 2.

3.4. Ranking of schemes

Here we propose a novel scheme ranking mechanism which is going to rank smart card based two factor authentication schemes and will help in determining the "*actual goodness*" of schemes in terms of a mathematical number which would be easy to

Table 2
Critical analysis Results of other schemes using Wang and Wang (2016) twelve criterion framework.

Criterion	Xie et al. (2017)	Wei et al. (2016)	Prabakar et al. (2019)	Sharma and Kalra (2018)	Cao and Huang (2013)	Mishra et al. (2015)
No verifier table	Meet	Meet	Meet	Meet	Meet	Meet
Password friendly	Does Not Meet	Meet	Meet	Meet	Does Not Meet	Meet
No password exposure	Meet	Does Not Meet	Meet	Meet	Meet	Meet
No smart card loss problem	Meet	Meet	Meet	Meet	Meet	Does Not Meet
Resistance to known attacks	Meet	Does Not Meet	Meet	Meet	Meet	Meet
Sound Repairability	Meet	Meet	Meet	Meet	Meet	Meet
Provision of key agreement	Meet	Meet	Meet	Meet	Meet	Meet
No clock synchronization	Does Not Meet	Meet	Does Not Meet	Does Not Meet	Meet	Does Not Meet
Timely typo detection	Does Not Meet	Meet	Meet	Does Not Meet	Meet	Meet
Mutual authentication	Meet	Meet	Meet	Meet	Meet	Meet
User anonymity	Meet	Meet	Meet	Meet	Meet	Meet
Forward secrecy	Meet	Does Not Meet	Meet	Meet	Meet	Does Not Meet

understand and calculate and would help in choosing the scheme more accurately.

The rationale behind putting forth a scheme ranking mechanism is that, if we are to ask as to which scheme is good then the most obvious answer would be the scheme satisfying all the twelve (12) criterions, which is indeed true in the ideal world but the not in the real world. Because, what if there are two schemes, one of which satisfies all the twelve criterions and the other scheme satisfies eleven criterions yet provide the same level of security? So it means that not all the criterions are of the same importance or type. If we look a little deeper, there are some criterions which are related to providing security while the other are responsible for a pleasant user experience and some both (subject to the design of the scheme). This indicates that we may have schemes that may not satisfy all the criterions yet are practical to use.

If we were able to associate a number or a rank to a scheme based on the goodness of schemes, then that would be very helpful. This would be especially useful for the top management in the company (which are mostly non-technical) during decision making as to which scheme is to be selected considering the cost, delivery timelines etc. To find out how the number can be given to a scheme, we have to come up with a scheme ranking mechanism that would truly communicate the real goodness and effectiveness of the scheme yet easy to calculate and understand.

By going through the Wang's criteria set and our earlier explanation of each of the criterion, we can break down the criteria set into three major categories which are as shown below in Table 3.

Now we can see from the above table that all the criterions in the "*Must Have*" category are related to providing robust security. While on the other extreme the "*May or May not Have*" category is purely dealing with user experience. The "*Nice to Have*" category has one criterion related to user experience which is sound repairability while the other is related to security. As mentioned earlier, clock synchronization is expensive to achieve and with the use of nonces in the scheme this can be achieved with relative ease and less cost. Since we are done with the categorization, we move towards the ranking of schemes. Now assigning equal weightage to each criteria is obviously counter intuitive since they are not of equal importance. So here we purpose the following weightage to each category and each criterion as below Table 4.

Table 3
Criterion categorization.

Sr. No	Category	Criteria
1	Must Have	C1 – No Password Verifier Table C2 – Password Friendly C3 – No Password Exposure C4 – No Smart Card Loss Attack C5 – Resistance to Known Attacks C7 – Provision of Key Agreement C10 – Mutual Authentication C11 – User Anonymity, C12 – Forward Secrecy
2	Nice to Have	C6 – Sound Repairability C8 – No Clock Synchronization
3	May or May Not Have	C9 – Timely Typo Detection

As can be understood from the above table that if we were to calculate how good a scheme is, we can use the weightages mentioned above and calculate the goodness of scheme. For example, if a scheme satisfies all the "Must Have" criterion and none of the remaining then the scheme scores 90%. If the scheme satisfies the first two categories, the score of the scheme would be 99% and so on. Since, the nine criterion of the first category are a must have so any scheme which is to be used for practical purposes should at least score 90%. An important point here is that if the scheme can achieve 90% without fulfilling one criterion from the first category still the scheme is not safe enough for practical implementation so we note here that scheme should score 90% or more including satisfying all the criterion of the first category. Thus we have developed a minimum threshold value with a condition which is shown in the below mentioned equation.

$$SEI \geq 90\% iffallcategory1criterionaresatisfied$$

Where SEI as we put forward the term for criterion satisfaction threshold stands for "*Scheme Effectiveness Index*" for smart card based two factor authentication schemes only. So now we can use SEI to actually plot a graph using the schemes analyzed by us. The graph is shown below Fig. 2.

Similarly, we can also plot SEI values of other schemes proposed over the years.

Below shown graph is depicting the average SEI value of schemes proposed over the years Fig. 3.

So we can see from the above graph that our proposed effectiveness index shows that over the period of 16 years the schemes,

Table 4
Criterion categorization.

Sr. No	Category	Weightage	Criteria
1	Must Have	0.1 Each	C1 – No Password Verifier Table C2 – Password Friendly C3 – No Password Exposure C4 – No Smart Card Loss Attack C5 – Resistance to Known Attacks C7 – Provision of Key Agreement C10 – Mutual Authentication C11 – User Anonymity, C12 – Forward Secrecy
2	Nice to Have	0.045 each	C6 – Sound Repairability C8 – No Clock Synchronization
3	May or May Not Have	0.01	C9 – Timely Typo Detection

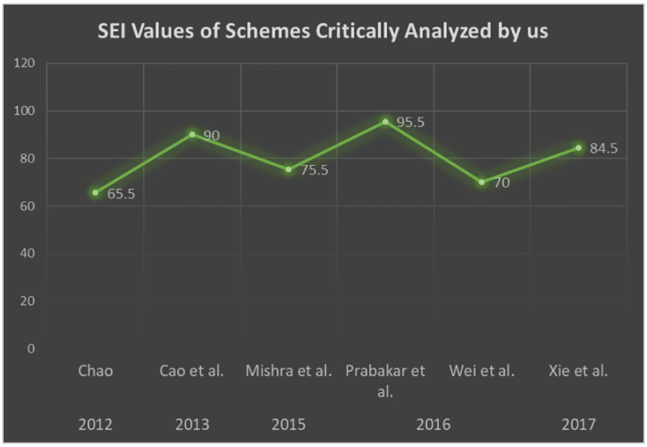

Fig. 2. SEI Values of other schemes critically analyzed using the framework.

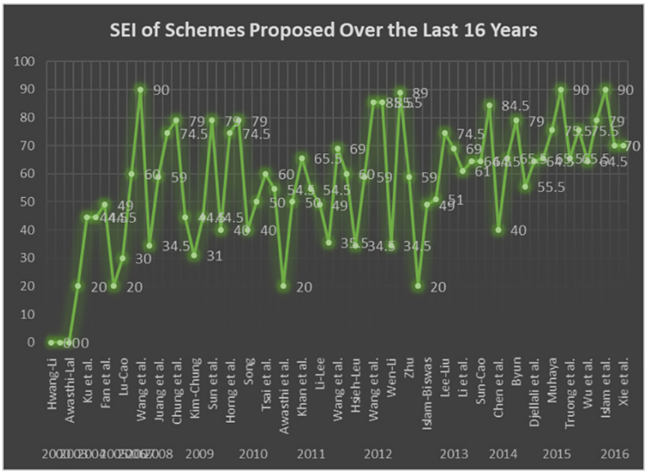

Fig. 3. SEI Values of schemes proposed over the last 16 years.

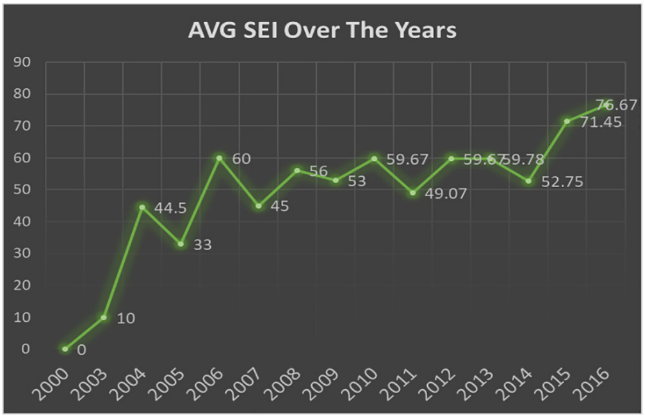

Fig. 4. Average SEI value over the years.

average value of SEI is showing an upwards trend which essentially means that proposed schemes are becoming more and more safer and compliant to the 12 criteria framework Fig. 4.

4. Conclusions, recommendations

So we have critically analyzed 6 recently proposed schemes using Wang's framework of 12 criterions and shown what are the weaknesses in those schemes. Furthermore, it is also established that Wang's proposed framework is indeed very comprehensive and well thought out to be used to critically analyze any further schemes that will be proposed in future. We also showed how one of the schemes namely Xie's et al. can be improved.

It is recommended to use Wang's proposed framework to critically analyze any smart card based two factor authentication schemes for single server environment only.

5. Future work

The future work includes the making of a criteria that can be used to critically analyze smart card based two factor authentication schemes proposed for multi-server environments since Wang's proposed criteria set is for schemes proposed for single server environments in which there is only one remote server and one control server however despite the increase in computational power and decrease in memory cost, yet it is important to cater multiple remote and control servers for redundancy and security purposes. Further, the users and servers would also somehow need to be aware of which user and server to contact for the protocol to work.

Acknowledgments

I would like to thank Almighty Allah SWT, Hafiz Mati-ur-Rehman, Dr. Khalid Hussain, Dr. Hasan Islam, Dr. NZ Jhanjhi my parents, siblings and my family for helping me and encouraging me to do this research. I am indebted for life.

References

Abdalla, M., Benhamouda, F., MacKenzie, P., 2015. "Security of the J-PAKE password-authenticated key exchange protocol,". In: Proc. IEEE S&P 2015. IEEE Computer Society, pp. 571–587.

Bonneau, J., Herley, C., Van Oorschot, P.C. and Stajano, F., 2012, May. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In Security and Privacy (SP), 2012 IEEE Symposium on (pp. 553-567). IEEE.

Camenisch, J., Lehmann, A., Neven, G., 2015. Optimal Distributed Password Verification. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, pp. 182–194.

Cao, T., Huang, S., 2013. Two-factor authentication schemes based smart card and password with user anonymity★. J. Comput. Inf. Syst. 9 (21), 8831–8838.

Chang, C.C., Wu, T.C., 1991. Remote password authentication with smart cards. IEE Comput. Digital Tech. 138 (3), 165–168.

Chen, B.L., Kuo, W.C., Wuu, L.C., 2012. Robust smart-card-based remote user password authentication scheme. Int. J. Commun. Syst. https://doi.org/10.1002/dac.2368.

J. Gosney, 2012, "Password cracking HPC," in Proc. Password, available at http://bit.ly/1y00I3O.

http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html.

https://duo.com/blog/four-years-later-anthem-breached-again-hackers-stole-employee-credentials.

https://www.scmagazine.com/report-dark-web-vendor-selling-millions-of-gmail-and-yahoo-accounts/article/645174/.

Liao, I.E., Lee, C.C., Hwang, M.S., 2006. A password authentication scheme over insecure networks. J. Comput. Syst. Sci. 72 (4), 727–740.

Madhusudhan, R., Mittal, R.C., 2012. Dynamic ID-based remote user password authentication schemes using smart cards: a review. J. Network Comput. Appl. 35 (4), 1235–1248.

Mishra, D., Chaturvedi, A., Mukhopadhyay, S., 2015. Design of a lightweight two-factor authentication scheme with smart card revocation. J. Inf. Security Appl. 23, 44–53.

Prabakar, M.A., Indrani, B. and Veni, M.K., Provably Secure Two-Factor Authentication Scheme For E-Health Using Smart Card.

Sharma, G., Kalra, S., 2018. A lightweight multi-factor secure smart card based remote user authentication scheme for cloud-IoT applications. J. Inf. Security Appl. 42, 95–106.

Sood, S.K., Sarje, A.K., Singh, K., 2010. An improvement of Xu et al.' s authentication scheme using smart cards. Proceedings of the Third Annual ACM Bangalore Conference, Bangalore, Karnataka, India, pp. 1–5.

Tsai, C.S., Lee, C.C., Hwang, M.S., 2006. Password authentication schemes: current status and key issues. IJ Network Security 3 (2), 101–115.

Please cite this article as: K. Hussain, N. Jhanjhi, H. Mati-ur-Rahman et al., Using a systematic framework to critically analyze proposed smart card based two factor authentication schemes, Journal of King Saud University – Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2019.01.015

Wang, Y., 2012. Password protected smart card and memory stick authentication against off-line dictionary attacks. Inf. Security Privacy Res., 489–500

Wang, D., Wang, P., Ma, C.G., Chen, Z., 2014. iPass: Robust smart card based password authentication scheme against smart card loss problem. J. Comput. Syst. Sci.

Wang, D., He, D., Wang, P., Chu, C.H., 2015. Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment. IEEE Trans. Dependable Secure Comput. 12 (4), 428–442.

Wang, D., Wang, P., 2014. On the anonymity of two-factor authentication schemes for wireless sensor networks: attacks, principle and solutions. Computer Networks 73, 41–57.

Wang, D., Wang, P., 2016. Two birds with one stone: Two-factor authentication with security beyond conventional bound. IEEE Trans. Dependable Secure Comput.

Wang, D., Gu, Q., Cheng, H., Wang, P., 2016. The request for better measurement: A comparative evaluation of two-factor authentication schemes. In: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. ACM, pp. 475–486.

Wang, R.C., Juang, W.S., Lei, C.L., 2011. Robust authentication and key agreement scheme preserving the privacy of secret key. Comput. Commun. 34 (3), 274–280.

Wei, J., Liu, W., Hu, X., 2016. Secure and efficient smart card based remote user password authentication scheme. IJ Network Security 18 (4), 782–792.

Weinshall, D., 2006. ''Cognitive authentication schemes safe against spyware,''. In: Proc. IEEE S&P 2006. IEEE, pp. 295–330.

Wu, T., 1998. ''The Secure Remote Password Protocol,''. In: Proc. NDSS 1998. The Internet Society, pp. 1–15.

Xie, Q., Dong, N., Wong, D.S., Hu, B., 2016. Cryptanalysis and security enhancement of a robust two-factor authentication and key agreement protocol. Int. J. Commun. Syst. 29 (3), 478–487.

Xie, Q., Wong, D.S., Wang, G., Tan, X., Chen, K., Fang, L., 2017. Provably secure dynamic id-based anonymous two-factor authenticated key exchange protocol with extended security model. IEEE Trans. Inf. Forens. Security 12 (6), 1382–1392.

Xu, J., Zhu, W.T., Feng, D.G., 2009. An improved smart card based password authentication scheme with provable security. Comput. Standards Interfaces 31 (4), 723–728.

Yang, G., Wong, D.S., Wang, H., Deng, X., 2008. Two-factor mutual authentication based on smart cards and passwords. J. Comput. Syst. Sci. 74 (7), 1160–1172.

Please cite this article as: K. Hussain, N. Jhanjhi, H. Mati-ur-Rahman et al., Using a systematic framework to critically analyze proposed smart card based two factor authentication schemes, Journal of King Saud University – Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2019.01.015