I. J. Computer Network and Information Security, **2019, 1, 47-61**
Published Online January 2019 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2019.01.05

A Critical appraisal on Password based Authentication

Amanpreet A. Kaur
Jamia Millia Islamia/Department of Computer Science, Delhi, 110025, India
E-mail: iamanpreetkaurcs@gmail.com

Khurram K. Mustafa
Jamia Millia Islamia/Department of Computer Science, Delhi, 110025, India
E-mail: kmfarooki@yahoo.com

Received: 07 November 2018; Accepted: 21 November 2018; Published: 08 January 2019

***Abstract*—**There is no doubt that, even after the development of many other authentication schemes, passwords remain one of the most popular means of authentication. A review in the field of password based authentication is addressed, by introducing and analyzing different schemes of authentication, respective advantages and disadvantages, and probable causes of the 'very disconnect' between user and password mechanisms. The evolution of passwords and how they have deep-rooted in our life is remarkable. This paper addresses the gap between the user and industry perspectives of password authentication, the state of art of password authentication and how the most investigated topic in password authentication changed over time. The author's tries to distinguish password based authentication into two levels 'User Centric Design Level' and the 'Machine Centric Protocol Level' under one framework. The paper concludes with the special section covering the ways in which password based authentication system can be strengthened on the issues which are currently holding-in the password based authentication.

***Index Terms*—**Password, Authentication, User Level Authentication, Machine Level Authentication, Cryptographic schemes.

I. Introduction

At present, identity theft is one of the most prevalent security threats. Consequently, the circumstances and prevailing context are pressing hard the need for effective-n-efficient authentication means. Authentication is an inevitable process of verifying an individual's identity, who wants to access the resources of a system. Though, machine authentication (machine-machine authentication) is to protect the machine through several secure protocols like Secure Socket Layer (SSL) but it cannot stop illegal accesses. In order, user authentications come to rescue, and we witness stringent policies to avoid identity theft. Every system has different authentication arrangements to involve different authentication techniques. The ultimate objective of authentication is to increase the security level of authorized users and to hinder the unauthorized access, whatsoever authentication technique is employed. The classification of authentication techniques is based on three zones: Knowledge Based Authentication (KBA), Object Based Authentication (OBA), and Characteristics Based Authentication (CBA).

Knowledge Based Authentication (KBA) includes user-id and password, passphrase, challenge questions, zero knowledge based protocols, challenge response protocols etc.

OBA is characterized by the physical possession or use of any hardware device used to authenticate the user such as smart cards, identity cards etc. It is employed generally in banking, transport, parking and hotels [1]. The difficulty of misplacing the device and granting unauthorized access can be solved by embedding other factors into it. CBA or Biometrics is characterized by unique property, a user possesses, including fingerprint, audio or voice recognition, signature recognition and face recognition. Kaur and Mustafa (2016) also discussed various authentication mechanism and authentication methods. Their respective strengths and weaknesses are briefly listed in Table I.

Password Based Authentication (PAS) is a type of Knowledge based authentication in which knowledgeable information such as passwords is kept as a secret from any other individual for access to a system [7]. Despite of the security problems, password authentication has a major influence on the internet for the last five decades. Several researchers have worked for strengthening password based authentication, primarily to enhance effectiveness. However, a few have tried various schemes for improving the efficiency - including changing the time computations, increasing the security considerations etc. Some authors tried to strengthened the passwords by increasing the time of computation to prevent brute force attacks. A new password scheme was derived by [8] by continuous iteration of hash function on the original master password. Manber [9] combined a random value known as "password supplement" to the password before

it is hashed.

Table 1. Strengths & Weakness of Typical Authentication Schemes

Authentication	**KBA** [3],[4]	**OBA** [1], [4]	**CBA** [4],[5],[6]
Weakness	Recall – memory burden, vulnerable to security attacks including collusion, guessing, lost credentials, dictionary attacks and brute-force attacks.	Objects can be shared or lost, additional cost required as it uses special input device, deploy-ability to other platforms is not easy.	Additional cost used for input device, False Accept Rate, False Reject Rate, Equal Error Rate, Failure to Enrol Rate and Failure to Capture Rate, not compatible with other platforms.
Strength	Easy to use, cost effective and ve0ry popular	Resist adversaries' attacks, No recall	No recall , Nothing to carry, most reliable

It appears that Bruce Schneier [10] rightly quoted that "If you think technology can solve your security problems, then you don't understand the problems and you don't understand technology". However, it is well known that human is the weakest link in the security chain. It has been studied that many users knowingly or unknowingly hamper security mechanism such as password based authentication. It is analyzed that this compromise can be a result of the implementation and understanding of mechanisms. Incidentally, it appears that more focus has been given to the technical aspects of the password based authentication ignoring the fact that it has to be handled by common people, may be a layman. Hitchings [11] and Davis and Price [12] also concluded that this results in less effective security mechanism. Ironically, human link has been studied more by hackers than the security designers; therefore, the security breaches are more usual. A closer analysis revealed that those who implement security need to communicate more with users to follow up with a user centered design [13]. Subsequently, it is generally echoed that organizations should focus on intelligence driven security model to prevent noise on the data hampering.

Majority of research have been done on easily formalized aspect of passwords (strict password policies, composition) rather than real world design tasks. There definitely appears a disconnect between what is causing a significant harm and what have been researched. Despite of these abundant issues, passwords are still a dominant form of user authentication. Hence, the focus rests on strengthening the password and its authentication. One of the pertinent and burning issues is to devise effective and efficient authentication as a whole and password especially therein, as password being an inevitable feature to authentication today.

II. Survey Methodology

In order to conduct systematic research, we collected the publications from relevant sources. Google Scholar, ACM Digital library and IEEE digital library were identified to collect the relevant papers. The keywords used for search were "Password Authentication", "User Authentication", "Password Security", "Password Authentication protocols", "Password design", and "Password Problems". A total of 506 papers were selected in order to critically review the literature for password authentication. Figure 1 elaborates the Research methodology as followed.

To evaluate the results of the review six research questions were framed:

R1: Which Journals frequently include papers on Password based authentication?

R2: What types of paper are published in the specified areas?

R3: What is the state of the art in the field of password based authentication?

R4: What are the most investigated password authentication topic and how these have changed over time?

R5: What are the prevailing problems in password based Authentication?

R6: What are the other relevant conclusive indications on password based authentication?

A. Results

R1: Which Journals frequently include papers on Password based authentication?

The following journals & conferences were recognized as the most relevant ones: "IEEE Security & Privacy", "ACM Transactions on Information and System Security", "Computers & Security", "IEEE transactions on computers", "International Journal of Information Security", "EEE Symposium on Security and Privacy", "International Conference on Security in Communication Networks", "International conference on World Wide Web ACM", "USENIX Security Symposium", "SIGCHI Conference on Human Factors in Computing Systems" and "ACM conference on Computer and communications security".

R2. What types of paper are published in the specified area?

According to our screening, topic related to passwords were divided into two levels based on the fact that they involve user or machine. Fig. II, also depicts the distinction between the two levels. What types of passwords user like, what should be considered while making password composition policies, which approach should be followed to avoid password theft? What types of cryptographic protocols have been used to efficiently store and pass the password avoiding different password attacks? Considering these as the factors for categorizing papers, following levels are identified.

- User – Machine Authentication (User-Centric Design Approach) – The first level caters the way a password is created & used by the user. Hence elements of passwords, password design, Password Composition Policies, Password Strength etc. fall under this category.
- Machine –Machine Authentication (Machine Centric Protocol Approach) - This level caters the way, how passwords are communicated from the client to the server. Protocols used for communication as well as their resistance to attacks falls under this category.

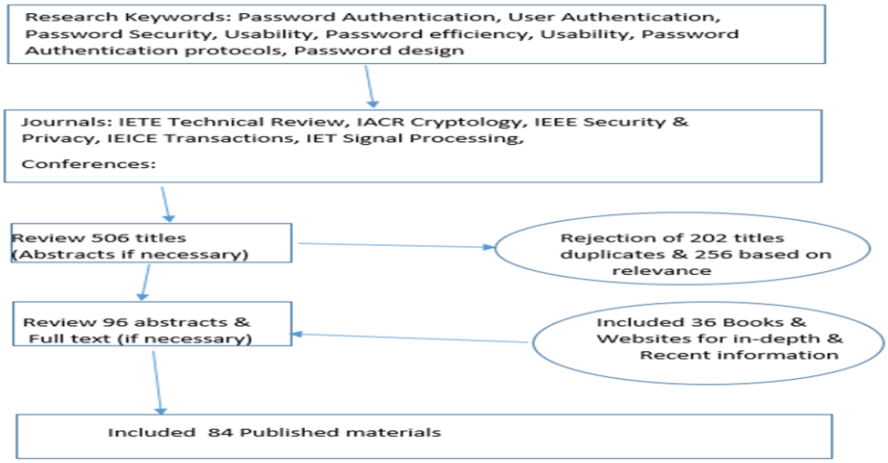

Fig.1. Reserch Methodology

R3: What is the state of the art in the field of password based authentication?

Since the inception of passwords in 1961, when the first computer password was built at Massachusetts Institute of Technology, we have come a long way since then. In 1962, the same system got his first security breach, as one of the user printed all the passwords from the file and handed over to other users. Such breaches, Called for the standardization of the security policies. Hence, in 1979 Data Encryption Standard (DES) was identified as the standard by National Bureau of standards. However, Electronic Freedom Foundation break down the DES key in 1998. In 1997, Advanced Encryption Standard (AES) was invented, which is still used today. Though passwords are plagued with problems, but deserve some praise also. More than two million users are using the internet services such as social networking, emails, banking and many more. They are primarily in use because of simplicity and cost-effectiveness, in comparison with other means of authentication. Whether it is account setup or revocation of password, it is an easy and less time consuming job. A simple browser can help us to access an account anywhere in the world. A smart user can incorporate a strong password for protecting itself from various attacks.

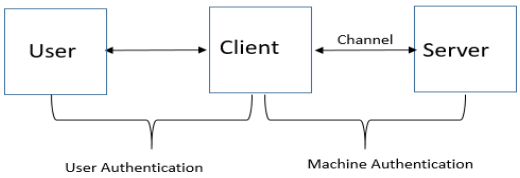

Fig.2. Different Levels of Password Authentication

No-one can deny the fact that passwords are one of the influential factors, which lead to the enormous growth of the internet. Whether it is Facebook or LinkedIn, passwords help these startups to grow, as the cost per user is almost negligible. Hence, we must accomplish this enticing record of passwords. Undoubtedly, passwords also offer certain advantages over other alternatives to authentication. Passwords are used to protect diversity of requirements ranging from a financial transaction to social networking sites. It is often seen that users are reluctant about the use of stronger authentication, as it puts in more cost and more effort, hence less usable. Largely service providers rely on the existing software obtained by the end users, which makes it difficult for alternatives that need special deployment. Table II discusses year by year advancements in password based Authentication. The later Section on Password Authentication Schemes will discusses more about the User centric approach and Machine Approach.

R4. What are the most investigated password authentication topic and how these have changed over time?

It has been observed that in the interval of 1970-1980, more focus was given to how passwords flow from one system to another or how to store them, in order to protect passwords from breach. In latter years' different approaches were used to effectively as well as efficiently pass the secret while resisting attacks [14]. However, passwords problems related to humans were still ignored in that era. However, in the beginning 1990's some researchers started to look for the weakest link in authentication[13].

Table 2. Categorization of the Topic According to the Time Intervals

Year	Topic	Sub-Topic
1970-1980	Machine-Machine Authentication	• Password Security [19]
1980-1990	• Machine-Machine Authentication • Password Problems	• One-way encryption [20] • Identity based Cryptosystem [21] • Public Key Cryptosystem [22] • Password Security [14] • Password Problems [7] • Timestamps [23]
1990-2000	• Machine-Machine Authentication • User Centric Design Approach	• Remote Smart Card Authentication [24] • Graphical Authentication through Recognition Based Scheme [25] • Keystroke Dynamics through Neural Networks [26] • Human as the weakest link [13] • Password Authenticated Key Exchange [27] • Password Security [28]
2000-2010	• Machine-Machine Authentication • User Centric Design Approach • Usability	• Graphical Authentication using Passpoints [29] • Keystroke Dynamics for cellphones [30] • Efficient Password Authentication using smart cards [31] • Usability & security of web Authentication [32] • Password Managers [33] • Password Security – Users centric [34] • Password Authentication and Group Diffie Hellman key Exchange [35] • Password Generators [36] • Password Quality [37] • Password Habits [38] • Website practices [39]
2010-2018	• Machine-Machine Authentication • User Centric Design Approach • Usability	• Comparative Evaluation of Passwords [4] • Keystroke Dynamics with Continuous verification [40] • Password Composition Policies ([16], [41] and [42]) • Efficient and Dynamic Smart Card Authentication ([43], [44]) • Digital Signature Algorithm using Elgamal [3] • Two Factor Authentication Improvement for wireless Sensor networks [44] • Multifactor Password Authenticated Key Exchange [45] • Round Optimal Password Authenticated Key exchange [46] • Wireless sensor Authentication [47] • Multimodal Biometric Person Authentication [6] • Password Authenticated Key Exchange with low resource Consumption [48] • Dynamic Combination of Authentication Factors [49] • Usability-Strengthening Password Based Authentication [50]

A lot of problems have been recorded with the way users were using passwords [7]. It's has been the lack of motivation, learnability and memorability that has been causing the security vulnerabilities. The usability and security tradeoff have been evaluated and many alternatives to replace passwords have been compared [4]. Still, passwords are inevitable. The change of focus from the technical to the design side will eventually help users to bridge the gap between what is expected and how is it expected. Table II will give us more insights towards the areas published under password authentication according to their time interval. The comparison between the time intervals clearly indicates that still most of the research is done on how we can make the machine to machine authentication efficient by the use of different levels, factors and algorithms. The comparison also made us realize that still we have efficient password protocols that save computation time & resources, but efficiency regarding user approach is still an open topic. This calls for another area for research which focus on Efficient User Centric Mechanism / Protocol/Framework.

The Results from the review indicates the categorization of the password authentication schemes into two streams. The later section will describe the levels in detail.

R5: What are the prevailing problems in password authentication?

Though, Password seems to be weak security mechanism, yet is an inevitable technique to the authentication world. Every user is being discouraged to use weak passwords, not to put it down on paper, not to be disclosed to anybody and not to be used for different accounts. Yet, it is a tendency to make it reusable feature otherwise they may have many passwords for multiple accounts resulting in high mental pressure. The main weakness comes due to the precise recall in the

knowledge based authentication that slightest error could make your authentication fail. Hence Perrig [15] suggested the use of recognition based authentication and implemented "Déjà vu". Inglesant and Sasse [16] studied that the designers should focus more on HCI design rather than password policies to strengthen password. Several researchers have contributed to the fact that there is a disarticulation between those who are not affected by the cost of security mechanism and to those who are affected by the security breaches [17]. Beautement, Sasse and Wonham [18] suggested that organizations should analyze costs and benefits to handle the downsides of security. Section on Password Problems & Solutions will discuss the prevailing problems & solutions in detail.

R6: What are the other relevant conclusive indications on password based authentication?

The foremost point the analysis indicates is that both the levels of authentication (Machine level, User level) has not been targeted fairly. Since, the inception of passwords, there is a lot of improvement on the technical aspects of password authentication. However, the user side of story still felt ignorant. Almost after two decades, since the passwords were used, the user problems got recognized [Table II]. The findings also suggest the gap between Who Make!! Who Enforce! and Who Follow! The last section on Conclusion will discuss the findings in detail.

III. Password Problems & Solutions

The main problem for the passwords is the gap between the usability and current tool support. There is a lack of connection between the user behavior and security mechanism. This can be a cause of avoidance to security mechanism [13]. Users should be given guidance related to their behavior rather than giving unrealistic guidance. Various problems that are associated with passwords are accounted as follows:

- Weak Passwords: It is clearly identified that the most common cause for cracking the system was weak passwords [52]. Trust wave 2012 Global security report, while analyzing the usage and weakness trends also revealed that it as a prime concern and that 80% of security incidents were due to the use of weak passwords.
- Memorability Issue: Passwords do rely upon precise recall of the secrets, which makes your system access fails even if the slightest of mistake occur.
- Reusability of Passwords - Users need to keep track of many accounts and passwords. Florencio and Herley [38] studied that a user on an average has about 25 password driven accounts. Handling so many accounts make the user to reuse the password to lessen the cognitive load.
- Password Composition Policies - When strict policies are enforced, the potency decreases and the weaker alternative measures are followed. This leads to frustration in users and huge cost both in terms of funds and resources of the organization [16].
- Database Leaks – Various websites have been a target of database leak revealing passwords of millions of users. Yahoo (2012) [54] and many more can be cited as examples of the leaks. This encourages the hacker to understand the know-how of the user passwords which indicates the style of the chosen passwords.
- Vandalism by Phishing and Key logging - Users are also facing the problem of key logging, when a system is infected with the malware and the password typed by the user is recorded by the attacker [16]. Phishing is also a common exercise where user did not understand that they are entering an impersonated system [55]

The solutions for the password problem can be generally formalized by recognizing the weAk passwords, implementing techniques to improve the reckoning part, and highlighting the security educaTion and awareness [15]. Some of prominent solutions deployed in the form of policies, mechanism, tools etc. are described briefly as follows:

- Dynamic Password Composition Policies: Different individuals or groups have different requirements. Flexible password policy that can calculate the risk faced by the user considered helpful to the customize password composition policies [16].
- Password Meters- The main problem of password is the password leakage due to the formation of weaker passwords. Strong enforcement policies make the user frustrated [56]. Hence password meters are a representation of the strength of the password and are usually depicted as a bar on the visual aid. Websites like twitter, Google involve the usage of password meters to aid the user for formation of stronger passwords. Stronger passwords are the result of a push given by password meters for important accounts and no observable difference is noted for unimportant accounts. We conclude that meter's result in stronger passwords when users are forced to change existing passwords on "important" accounts and that individual meter design decisions are likely have a marginal impact [57].
- Password Mangers: These are used to protect web accounts from unauthorized access, maintain strong passwords that are not vulnerable to different attacks but are easy to remember by the use of some cryptography protocols. They also intend to reuse the password across different web accounts by involving some salts. Browser extensions such as PwdHash is an example of such types [33].
- Password Generators: The creation of stronger passwords is facilitated with the help of password generators. It had been founded that at times password meters and generators have been a victim

of third party attacks [58]. Password meters transmit the password information to the third party websites via JavaScript. It is also studied that account registration pages do no rely on password meters and most of them leak the credentials [58].

- Out of band Password Authentication: It not only solves the password management problem but also hampers the malware running on the system to get away with the user credentials. The authentication from the service provider is handled by the mobile devices as the username and passwords are stored in the encrypted manner in the mobile devices. After the establishment of the session, the mobile devices transfer it to the system. So the user did not enter their credentials on their system, from where malware can steal it [59].
- Two Factor Authentication: It is said to be an incremented model of authentication where a second form of authentication adds to the level of security. The users who have been a victim of password stealing can move to the two factor authentication as it will enhance the security conditions by controlling the second authenticator if one of them is compromised.
- Single Sign-on: It is another solution for password problem where authentication is done only once for multiple websites. Hence, the memorability issues are somewhat tackled. Facebook, twitter and open Id are examples of single sign on entities.
- Keystroke Dynamics - is a low cost behavioural biometrics applied to access and measure unique typing rhythm by monitoring the digital devices such as mobile phone, touch screen panel or keyboard. This generally does not need any extra devices which make it suitable and cost effective [60]. One of the advantages of this approach is strengthening conventional password Authentication. Its adds up to an extra layer of security by increasing reliability of biometrics to the simplicity of password scheme.

IV. Password based Authentication Schemes

Password based authentication can be primary segregated into two Levels – User Centric Approach and Machine Centric Approach (Fig II). Machine to machine password exchange can be considered as protocol based authentication scheme or Machine Centric Approach, whereas secure password entry in user to machine frames is the criteria for User Centric Approach or design based authentication schemes. Improvement in both the levels can make the authentication efficient as well as effective. Hence to strengthen the authentication model we have to categorize it in two levels: Machine- Machine Authentication and secondly User Centric Authentication. The above mentioned schemes are described briefly in the following section. A detailed classification is mentioned in Fig. II.

A. User Centric Design Scheme

A recent survey conducted by government-commissioned PwC information security found that on an average between £1.46m to £3.14m had been the cost of data breach of more than 90% large enterprises [61]. In future, a portal that will generate secure password based on the data imported from active directory may surely enhance security and save time [62]. Password management solutions or design solutions that are easy to use can increase the transparency and visibility by increasing the password security. So, the User centric scheme revolve around how users use passwords. So, to understand the approach, we started by explaining the password elements, their design, password composition policies and their corresponding strength.

1. Elements of Password Authentication

Generally, an authentication process as is based on the following five elements: user seeking authentication, distinguishing characteristics for authentication, the authenticator, the authentication mechanism - input, transportation system and verifier - and access control mechanism. However, from the physical perspective following elements have been prominently and consistently in use.

- Alphabet Classes-It is defined as the different sets of characters given in the choice set. For example, some passwords demand three sets of classes, one alphabet, special symbols and numeric [39].
- Alphabet Size-It is described as the number of characters; the user has to choose from the alphabet class. For example, if the user chooses the decimal class, the alphabet size will be of length 10 (0-10) ([37], [63])
- Password Length- ¬It is defined as the number of characters needed to fulfill the requirement of a valid password. Password length has a direct impact on the character space of the password as it is related to the possible combination of the password [39].
- Authentication Period- It is described as the time span and the actions which results into the grant of access i.e. for which period the process is valid. For example, intra session, multiple sessions [63].
- Input Visualization- It is the criteria for the user receiving the feedback from the system for the characteristics of password chosen. For ex plaintext, encrypted text etc. [64].
- Lifetime- It is described as the timeframe for which a password is stated as valid. After the expiration of the lifetime, the password is no longer used for authentication and a new password should be issued /changed for authentication purposes [39].
- Password Guidance-It depicts how much support is provided to the users for selecting a password. For example, none, minimum selection tips etc. [39].
- Generator of Password- The source which generates the password of the system is the entity responsible for the enforcement of password regulation. The generator can be the user or the System security

officer or the password mechanism itself [7].
- Storage- Password mechanism store the username/password information in a file, in a non-file, or in an another system [7].

2. *Password Design*

During the last five decades, passwords had a significant impact on authentication despite of their security issues. Traditional passwords are commonly used in any operating system, where each user is allowed to generate a user-id and password known only to him who acts as an authenticator. Generally, users tend to choose easily guessable passwords [4] and make it a habit to reuse the same passwords among multiple accounts [38]. Many warnings and guidelines have been given to the users to avoid writing down their passwords to mitigate their misuse ([16],[34] and [28]). Passwords that are not written down are not that stronger; and hence result in security compromise. Hence, Organizations should maintain a balance for regulating the password policies between memorability issues and security breaches [14].

As passwords are more prone to security breaches, the common condition is the formation of weak passwords. Users commonly make this mistake, when they create the password on their own. Following are the prevalent alternatives to choose the formation of passwords by other means:

- System Generated Passwords- These are randomly picked string of characters generated by the authentication system, which are surely difficult to guess and difficult to remember [36].
- Associative Passwords- These are cue –response types of passwords that are unique to an individual [65]. In order to make the scheme stronger the word association should be non-trivial.
- Cognitive Passwords-These are the question – answer type of passwords, also known as challenge-response scheme. A user has to provide several passwords instead of one to get the access [28]. The question may be personal to that individual hence should be non-trivial.
- Passphrases - It is also a type of password composite of sequence of words. They are longer than the traditional password but don't take much issue on memory. Many institutions had welcomed the idea of passphrases [66] going by the empirical studies.

3. *Password Composition Policies*

It is studied that good password composition policies makes up strong password but t increases the memory load also [67]. The set of requirements that are framed by password composition policies also makes the password difficult to guess [68]. Following are the different techniques used prominently by the organizations for password composition.

- Rule-based Approach: This is the traditional approach in which some sort of rules such as minimum and maximum letters, special character, spaces are predefined. After researching, many authors have formulated that this technique is ineffective (Weir et. al, 2010).
- Random Approach: System generated passwords are randomly generated strings, set as passwords, which are not easily memorable. Hence it poses problems for the users as random passwords are difficult for the users to remember [69].
- Analyze-Modify Approach: It is one the new techniques through which we can create strong passwords without interrupting the usability factor. It strengthens the passwords by the use of probabilistic approach. The model initially checks whether the password is strong or not by estimating the entropy of the password and then applies context free grammar in order to strengthen the password [42].

4. *Password Strength*

The strength of the password is estimated by the time; an algorithm takes to generate the guesses. If an attacker takes longer to break the password, the stronger is the password is. So, initially length of a password was often termed as a factor that influences the strength of a password. In [70] the author describes the password quality and entropy as a measure of password strength. Entropy values can be calculated by the summation of the length of the password, ordering of the character, total number of character type and the content of the character [41]. Entropy can also be used for filtering weak passwords for improvising dictionary checking [71]. A password quality indictor was developed by [37], using the time taken by trial and error method to find the correct password.

Table 3. Cryptographic Protocol based Scheme

Classification	**Public Key cryptographic protocols** ([77], [78],[79],[48],[80],[81])	**Hash function based Protocols** ([82],[83],[84],[85],[86],[45],[87],[3])
Protocols	RSA , Diffie Hellman protocol, Elliptic Curve cryptography	Hash Functions ex-XOR
Problems	Replay attacks, spoofing attacks, user masquerading, impersonation, clogging effect, insider attack	offline password guessing attack, replay attack ,server spoofing attack, stolen verifier, forgery attack
Inefficiency Cause	Complex Equation, memory overhead	Not provided key agreement and mutual authentication
Improvement	Nonces, encryption	Less mathematical operations, Hashed passwords, intensive modular exponentiation, timestamps

Thus, the measures for password quality were length of the password, range of the character set and its variation from dictionary. Password meters can be described as a measure for motivating users for making passwords strong. Suggestions are given to the users for employing stronger passwords by the means of password meters. It is also seen that the strength of the password is also influenced by the password meters [57].

B. Machine Centric Protocol Scheme

Finding out our way from the regime of weak to strong authentication, we traversed through the simple transmission to challenge response mechanism. The password is transmitted clearly in the form of text or image in simple transmission. In challenge response mechanism in accordance with the server authentication instance, a secret function is computed that enhances the freshness of the authentication but was vulnerable to online password guessing attacks.

Moreover, challenge response mechanisms can be further classified into challenge-response identification protocols based on symmetric-key techniques, public-key techniques, and zero-knowledge proofs [72]. While progressing to strong authentication i.e. from passwords to challenge response protocol, one time passwords offered partial solution to the problems accompanied by fixed passwords scheme. One time passwords were derived from the challenge response mechanism but have the unique property of "non-reusability" i.e. different passwords at every authentication session [21]. In asymmetric scenarios such as remote application where client is unable to possess a laptop or smart card, it uses its own human memorable weak password and server stores a long secret (private key). Gong et .al [73] initially tried the use of public key techniques with the combination of password protocols in order to protect weak passwords from offline guessing attacks via public key encryption.

The main drawback of simple password protocol was that the password or the hashed password was stored in the password table which has to be prevented from the intruders, so that the password is not revealed. Kehne et al [74]; Neuman, and Stubblebine [75] and Syverson [76] used the authentication protocols to ensure the security by using a trusted third party. However, they are still vulnerable to attacks as the secret keys are stored on the password tables.

To overcome the drawback of password tables, ID based schemes were introduced [88] in combination with smart cards [24]. ID based scheme offered many advantages over previous schemes. Firstly, no keys are need to be exchanged neither public nor private key. Secondly, it removes the password tables; and lastly no trusted parties are needed. The ID based scheme was not suitable for network environment as the concept of timestamps [23] was not included and was not resistant to replaying previously intercepted signature attack. Shiuh-Jeng, and Jin-Fu [89] employed the concept of timestamps on the Based on Elgamal's (ElGamal, 1985) and Shamir's ID-based schemes (Shamir, 1984).

However, these schemes also suffer some drawback, as not being fully resistant to replay and impersonation attacks, as the identities are not included in ID based scheme. Moreover, no password change option was there after registration. Yang, and Shieh, [94] solved the security problems arrived in ([88], [89]) by proposing a time-based scheme, which is helpful in an environment where clocks are synchronized such as our local area and needs only one message for authentication. Whereas a network where synchronization is not possible such as wide area network, satellite communication is proposed to be based on a scheme where three messages for authentication are needed.

Authentication protocol can be classified into two main categories based on their technique of message passing-Public key cryptography based [90] and Hash-based [91]. Respective problems faced by the cryptographic protocol and their cause have been identified and the proposed improvement has been described in Table III.

However, some features added functionalities beyond simple authentication. Password authentication protocol needs to accompany these features to use it for higher level application, described briefly as follows:

- Mutual Authentication: It is a two-way communication where a server authenticates the user and vice versa. It prevents the occurrence of attacks in remote situation where trust to the server is always questionable. Man in the middle attack and impersonation attack can be eliminated by the implementation of the same.
- Authenticated Key Exchange: A session key is shared between the server and the user at the end of every protocol. This session key is used to encrypt the messages transferred in the session. This feature prevents the data forgery and data hijacking.
- User Identity Protection: The identity of the user is not compromised having this feature and is useful in the application where remote authentication is needed.

The computation time of hash functions and exponential function is less than the multiplication/division and keys operations. Hence, the protocols using hash functions usually win over the time span as it reduces the time of computation. Whereas, protocols using the public key cryptosystem win over the security requirement by enabling mutual authentication through key agreement and are resistant to many attacks.

Device based protocols are designed to resist attack on password tables. The legitimate user can change the contents or destroy the password table which can lead to system breakdown. Moreover, the size of the password table is proportional to number of users employed. Hence, as the network increases the password table size also increases, which is difficult to maintain in large networked environment. Protocols used for password based authentication schemes can be further classified by the devices used with i.e. password only protocols, dedicated device aided PA protocols (e.g. smart card) and

memory device aided PA protocols (e.g. SB) [49].

1. Password Only Protocols

The protocols using password-only need only a login-id and a password to login into a system [92]. It is the basic authentication level and server needs a verification file to match the id, and password with an upcoming request. The maintenance of the verification file introduces the risk of hampering the file. Password authenticated key exchange protocols are designed for security even if user chooses short passwords. KOY protocol can be taken as an example of the same [93]. The following section briefly describes the password based authenticated key exchange and its types.

- Password-Based Authenticated Key Exchange: Authenticated Key exchange protocols allow several parties to share a common session key over insecure networks holding low entropy secrets such as passwords. Bellovin and Merritt [27] were the first to introduce PAKE. SPEKE and EKE introduced by Jablon [92] and Bellovin and Merritt [27] are probably the first and the best PAKE protocols known. They authenticate the two parties, offering resistance to offline attacks and posing restrictions on the number of attempts to resist online attacks. PAKE protocols also solve the problem of password leakage as it does not require Public Key Infrastructure to securely transfer the passwords through secure TLS channel. Apart from [95], [96] proposal offers several rounds of messages for communications. However, the works of Katz and Vaikuntanathan [47] and Benhamouda et al. [97] requires only one-round of communication.
- Tag-based Password Authentication: Manulis et al., [98] introduced the notion of tag-based Password Authentication (tPAuth) that performs mutual authentication instead of key exchange phase in PAKE. It is also used in Password Authenticated and Confidential Channel Establishment (PACCE) protocols by the help of that embedded tag tPAuth. An alternative of using the session key to establish secure and confidential channel is to bind a confidential channel to a password-based authentication protocol and hence, authenticate the confidential channel using the password.
- Three-Party Password Authenticated Key Exchange: [99] introduced three -party security model. A trusted server is allowed to share the password with the two parties who want to communicate. Further, authors Tsai and Chang [100] and Yoneyama [101] proposed improved protocols security models.
- Group Password Authenticated Key Exchange: It is an extension to the two party PAKE. A negotiable session key is shared between groups of people. It is primarily implemented through general group key exchange settings and changed for password settings [35].
- Multi-Factor Authenticated Key Exchange: Combating several authentication techniques into one technique enjoys the privileges and enhanced security of different techniques. Such techniques are often named as multifactor authentication. Starting from two, it contains up to three, four and many more levels of security. Some authors [46] have researched the area and proposed such models.
- Password Protected Secret Sharing: It shares a secret key split it into multiple servers, protected by a password. Remote storage is the most important application of this protocol. Similarly, hidden credential retrieval [102] use only one server to store high entropy messages. It was introduced as password authenticated recovery of secret data by Ford and Kaliski,[103] in the assumed public key infrastructure using only in secret sharing. Bagherzandi [104] improvised the concept with fewer complexities than other threshold password authenticated key exchange.

2. Dedicated Device Protocols

The second type of protocols needs a dedicated device like a smart card to authenticate a user. The external device is used to store the authentication information and is extracted using a specialized reader. The information contained in the device can also be hampered by monitoring the power consumption of the device regardless of being tamper resistant [105] Using tamper resistant devices increases the deployment cost and calls up for more security against stolen card attack and many traditional attacks. Smart cards can be used in conjunction with different cryptographic protocols for authenticating the user to a higher level of security. Dedicated devices can be used with different cryptographic protocols under different situations. Following is the related work under which smart card can be used with different protocols like RSA, Elgamal and hash based scheme [106]

- RSA Based Schemes: RSA is widely known as one of the public key cryptosystem. [94] proposed a RSA based authentication system which allows the user to freely choose their passwords and no verification tables are used to store the passwords. The authors Chan and Cheng (2001) found out that the Yang and Shieh timestamp based scheme was not [94] resistant to forgery attack. Further Yang, Wang, and Chang [107] modified the scheme which was not vulnerable to the previous attacks. Sun etc. Al [108] further stated the flaws of Liu, Zhou and Gao [109] scheme whereas impersonation attack poses a serious attack, as the server or the client can be cheated without having a secret information. Later, Ramasamy and Muniyandi [44] proposed a password based authentication mechanism which can resist most of the attacks with the application of RSA and smart card. The overhead storage is reduced as the server need not maintain any password tables, only time of registration is to be updated. Some prominent schemes are described as

follows:

- ELGAMAL Based Scheme: In 2000, [110] Hwang and Li proposed a password based authentication scheme based on Elgamal Public key cryptosystem. This system only used one secret key and its complexity lies in the discrete complexity over finite fields. No password table was required for remote authentication to check the identity of the user. This scheme was resistant to message replay attacks but vulnerable to impersonation attack. A digital signature algorithm was proposed by Chen, Shen and Lv [3] similar to ELgamal scheme, which form up with better security and less computational overhead. Moreover, with time new versions of Elgamal schemes came up which were conjured with discrete logarithm and digital signature by Diffie Hellman [111].
- Hash based Scheme: Peyravian and Zunic's [82] suggested a simpler authentication mechanism which used only a hash function to increase the efficiency but suffered from offline password guessing attack. Later, Hwang and Tzu-Chang [83] improvised the earlier version of Peyravian scheme still suffered from replay attack and server spoofing attack. Wong et al [84] proposed an authentication protocol based on hash function. It involves less mathematical operations as compared to cryptographic protocols. In 2010 Khan et al. [45] made significant changes to the DAS scheme [85] by using hashed passwords instead of using direct passwords but were vulnerable to replay and forgery attacks. It also overcomes the problems of wang et al [112] scheme which does not provide user anonymity during authentication. Moreover, it does not provide procuration of stolen smart card; neither user was allowed to change their passwords. In 2010, Baboo and Gokulraj [43] proposed a dynamic authentication scheme which comprises of all five essential components of information security- the authentication, confidentiality, reliability, integrity and security.

3. Memory Aided Protocols

The third type of protocols use a memory device aided password authentication protocol to save the deployment cost of tamper resistant dedicated device. It uses USB sticks, PDA's and mobile phone to store the common information needed for authentication, which may not be tamper resistant. The goal was to ensure the authenticity of data even if the memory device is stolen Jiang et al [87]. An insight to the protocols driven by the devices used with the password is described hereafter in the Table IV.

Table 4. Device based Protocols

Classification	**Password only protocols** ([93], [90])	**Dedicated device Protocols** [90], [91]	**Memory device aided Protocols** [87]
Authentication Mechanism	Login-id and password]	Smartcards	USB Sticks, PDA's, mobile phone
Protocols Used	PAKE [KOY], SPEKE and DH-EK	DE-PAKE(device enhanced –PAKE)	CDHP
Resistance against	Offline dictionary attacks, on-line dictionary attack, Provide mutual authentication.	Offline dictionary attacks(if device is not stolen), on-line dictionary attack	Offline dictionary attacks, on-line dictionary attack, Provide mutual authentication.

V. Conclusions

Users are known to be the weakest link in the authentication model, but they are the most troublesome component to the model too. The paper addresses the issue of who is developing the system and who is using it? The main contribution of this paper is analyzing this gap and reducing it by integrating the user view as design phase and developer view as protocol phase. The main problem for the passwords is the gap between the usability and current tool support. Rather, passwords are taken as a feature for sharing information. Stronger passwords are result of a push given by password meters for important accounts and no observable difference is noted for unimportant account. Hence, it can be suggested that it is not only the tools which are resulting in stronger security mechanism but the importance or relevance of the information which the user wish to protect Users should be given guidance related to their behavior rather than giving unrealistic guidance. Leaving the well specified format of problems, more research should be done on the design goals of the system taking care of efficiency and effectiveness of the system. If we are using intensive modular exponentiation, we should use more levels of protection as single level modular exponentiation can cause clogging effect. Factors may be added according to the situations to strengthen the security of the system. Holistic password policies through Out of band authentication may help users need not memorize the passwords which enable them to use strong passwords. Following are the two major findings that can also be directed as future direction for researchers:

- Strengthening Password Based Authentication

Several researchers have worked for strengthening password based authentication, primarily to enhance effectiveness. However, a few have tried various schemes for improving the efficiency - including changing the

time computations, increasing the security considerations etc. Some of the pertinent works traced around it are described briefly as follows.

It is apparent that we can strengthen the existing password based mechanism by improvising the two aspects of password security. First by strengthening the password protocols used in order to prevent online attacks and second by making the password entry strict to prevent offline attacks by strengthening the design mechanism of password based authentication [51]. A hash function is used to compute strong passwords maintaining the memorability by just memorizing a short password. Client functioning is used in this mechanism; hence no changes on the server side are used. It is resistant to brute force attacks and the user can compute the password regardless of the location [113]. Another approach for strengthening Password Authentication is Keystroke Dynamics. Irdus [114] also proposed keystroke dynamics to avoid the problems generating through password based authentication. The key timings can be can be measured by accessing their timing patterns and pressure sensors. The most popular timing measurement of keystroke input are Dwell Time(DT) and Flight Time(FT). Czeski et. Al [115] proposed a system where we can reap the benefits of passwords as well as security of second level authentication. Firstly, a user device (personal phone) can communicate with the user's system and then accordingly the server defends different policies depending on whether the user is using his personal device or not. Therefore, a layered approach for security is followed. Han et Al. [50] also combined different authentication factors based on risk and benefit policies. An adaptive mechanism was followed which is ordered with historical data to measure risk and benefit.

- Who Make! Who Enforce! Who Follow!

There is a disconnect between what is causing a significant harm & what has been researched. There is a lack of connection between user behavior & security mechanism. Users should be given guidance related to their behavior rather than giving unrealistic guidance. Designers should focus on HCI design rather than strong password composition policies. Organizations should analyze cost & benefits to handle the downside of security. The comparison also made us realize that still we have efficient password protocols that save computation time & resources, but efficiency regarding user approach is still an open topic. This calls for another area for research which focus on Efficient User Centric Mechanism / Protocol/Framework.

There is a difficulty to manage security and usability problems, hence it's worthwhile to give up elaborate password rules and look up for something good ones. It is high time to invest on strengthening efficiency aspect, without compromising effectiveness and security aspects.

REFERENCES

[1] Bruns, R., Dunkel, J. and von Helden, J., 2003. Secure Smart Card-Based Access to an E-Learning Portal. In ICEIS (4) (pp. 167-172).

[2] Kaur, A. and Mustafa, K., 2016, March. Qualitative assessment of authentication measures. In Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on (pp. 694-698). IEEE.

[3] Chen, H., Shen, X. and Lv, Y., 2010. A New Digital Signature Algorithm Similar to ELGamal Type. J. Softw, 5, pp.320-327.

[4] 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.

[5] Gil, C., Castro, M. and Wyne, M., 2010, October. Identification in web evaluation in learning management system by fingerprint identification system. In Frontiers in Education Conference (FIE), 2010 IEEE (pp. T4D-1). IEEE.

[6] Sahoo, S.K., Choubisa, T. and Prasanna, S.M., 2012. Multimodal biometric person authentication: A review. IETE Technical Review, 29(1), pp.54-75

[7] Jobusch, D.L. and Oldehoeft, A.E., 1989. A survey of password mechanisms: Weaknesses and potential improvements. part 1. Computers & Security, 8(7), pp.587-604.

[8] Kelsey, J., Schneier, B., Hall, C. and Wagner, D., 1997, September. Secure applications of low-entropy keys. In International Workshop on Information Security (pp. 121-134). Springer Berlin Heidelberg

[9] Manber, U., 1996. A simple scheme to make passwords based on one-way functions much harder to crack. Computers & Security, 15(2), pp.171-176.

[10] Schneier, B., 2011. Secrets and lies: digital security in a networked world. John Wiley & Sons.

[11] Hitchings, J., 1995. Deficiencies of the traditional approach to information security and the requirements for a new methodology. Computers & Security, 14(5), pp.377-383.

[12] Davis, D. and Price, W. Security for Computer Networks. Wiley, Chichester, 1987

[13] Adams, A. and Sasse, M.A., 1999. Users are not the enemy. Communications of the ACM, 42(12), pp.40-46.

[14] Wood, C.C., 1983. Effective information system security with password controls. Computers & Security, 2(1), pp.5- 10.

[15] Perrig, A., 2000, September. Shortcomings of password-based authentication. In 9th USENIX Security Symposium

[16] Inglesant, P.G. and Sasse, M.A., 2010, April. The true cost of unusable password policies: password use in the wild. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 383-392). ACM.

[17] Albrechtsen, E. and Hovden, J., 2009. The information security digital divide between information security managers and users. Computers & Security, 28(6), pp.476-490.

[18] Beautement, A., Sasse, M.A. and Wonham, M., 2009, August. The compliance budget: managing security behavior in organizations. In Proceedings of the 2008 workshop on new security paradigms (pp. 47-58) ACM.

[19] Morris, R. and Thompson, K., 1979. Password security: A case history. Communications of the ACM, 22(11), pp.594-597.

[20] L., 1981. Password authentication with insecure communication. Communications of the ACM, 24(11), pp.770-772.

[21] Shamir, A., 1984, August. Identity-based cryptosystems and signature schemes. In Workshop on the Theory and Application of Cryptographic Techniques (pp. 47-53). Springer Berlin Heidelberg

[22] ElGamal, T., 1985. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE transactions on information theory, 31(4), pp.469-472

[23] Denning, D.E. and Sacco, G.M., 1981. Timestamps in key distribution protocols. Communications of the ACM, 24(8), pp.533-536.

[24] Peyret, P., Lisimaque, G. and Chua, T.Y., 1990. Smart cards provide very high security and flexibility in subscriber's management. IEEE Transactions on Consumer Electronics, 36(3), pp.744-752.

[25] Dhamija, R. and Perrig, A., 2000, August. Deja Vu-A User Study: Using Images for Authentication. In USENIX Security Symposium (Vol. 9, pp. 4-4).

[26] Ahmad, A.M. and Abdullah, N.N., 2000, September. User authentication via neural network. In International Conference on Artificial Intelligence: Methodology, Systems, and Applications (pp. 310-320). Springer, Berlin, Heidelberg.

[27] Bellovin, S.M. and Merritt, M., 1992, May. Encrypted key exchange: Password-based protocols secure against dictionary attacks. In Research in Security and Privacy, 1992. Proceedings. 1992 IEEE Computer Society Symposium on (pp. 72-84) IEEE

[28] Zviran, M. and Haga, W.J., 1999. Password security: an empirical study. Journal of Management Information Systems, 15(4), pp.161-185.

[29] Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. and Memon, N., 2005, July. Authentication using graphical passwords: Effects of tolerance and image choice. In Proceedings of the 2005 symposium on Usable privacy and security (pp. 1-12). ACM.

[30] Campisi, P., Maiorana, E., Bosco, M.L. and Neri, A., 2009. User authentication using keystroke dynamics for cellular phones. IET Signal Processing, 3(4), pp.333-341.

[31] Kumar, M., 2004. On the Weaknesses and Improvements of an Efficient Password Based Remote User Authentication Scheme Using Smart Cards. IACR Cryptology ePrint Archive, 2004, p.163.

[32] Renaud, Karen. "Quantifying the quality of web authentication mechanisms: a usability perspective." Journal of Web Engineering 3.2 (2004): 95-123.

[33] Chiasson, S., van Oorschot, P.C. and Biddle, R., 2006, August. A Usability Study and Critique of Two Password Managers. In Usenix Security (Vol. 6).

[34] Riley, S., 2006. Password security: What users know and what they actually do. Usability News, 8(1), pp.2833-2836.

[35] Bresson, E., Chevassut, O. and Pointcheval, D., 2007. A security solution for IEEE 802.11's ad hoc mode: password-authentication and group DiffieHellman key exchange. International Journal of Wireless and Mobile Computing, 2(1), pp.4-13.

[36] Leonhard, M.D. and Venkatakrishnan, V.N., 2007, May. A comparative study of three random password generators. In Electro/Information Technology, 2007 IEEE International Conference on (pp. 227-232). IEEE

[37] Ma, W., Campbell, J., Tran, D. and Kleeman, D., 2007. A conceptual framework for assessing password quality. International Journal of Computer Science and Network Security, 7(1), pp.179-185.

[38] Florencio, D. and Herley, C., 2007, May. A large-scale study of web password habits. In Proceedings of the 16th international conference on World Wide Web (pp. 657-666). ACM.

[39] Furnell, S., 2007. An assessment of website password practices. Computers & Security, 26(7), pp.445-451

[40] Shimshon, T., Moskovitch, R., Rokach, L. and Elovici, Y., 2010, December. Continuous verification using keystroke dynamics. In Computational Intelligence and Security (CIS), 2010 International Conference on (pp. 411-415). IEEE.

[41] Komanduri, S., Shay, R., Kelley, P.G., Mazurek, M.L., Bauer, L., Christin, N., Cranor, L.F. and Egelman, S., 2011, May. Of passwords and people: measuring the effect of password-composition policies. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 2595-2604). ACM

[42] Houshmand, S. and Aggarwal, S., 2012, December. Building better passwords using probabilistic techniques. In Proceedings of the 28th Annual Computer Security Applications Conference (pp. 109-118). ACM

[43] Baboo, S.S. and Gokulraj, K., 2010. A secure dynamic authentication scheme for smart card based networks. International Journal of Computer Applications, 11(8), pp.5-12.

[44] Ramasamy, R. and Muniyandi, A.P., 2012. An Efficient Password Authentication Scheme for Smart Card. IJ Network Security, 14(3), pp.180-186.

[45] Khan, M.K. and Alghathbar, K., 2010. Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks'. Sensors, 10(3), pp.2450-2459.

[46] Stebila, D., Udupi, P. and Chang, S., 2010, January. Multi-factor password-authenticated key exchange. In Proceedings of the Eighth Australasian Conference on Information Security-Volume 105 (pp. 56-66). Australian Computer Society, Inc

[47] Katz, J. and Vaikuntanathan, V., 2011, March. Round-optimal password-based authenticated key exchange. In Theory of Cryptography Conference (pp. 293-310). Springer Berlin Heidelberg.

[48] Yeh, H.L., Chen, T.H., Liu, P.C., Kim, T.H. and Wei, H.W., 2011. A secured authentication protocol for wireless sensor networks using elliptic curves cryptography. Sensors, 11(5), pp.4767-4779.

[49] Qian, H., Gong, J. and Zhou, Y., 2012. Anonymous password‐based key exchange with low resources consumption and better user‐friendliness. Security and Communication Networks, 5(12), pp.1379-1393

[50] Han, W., Sun, C., Shen, C., Lei, C. and Shen, S., 2014. Dynamic combination of authentication factors based on quantified risk and benefit. Security and Communication Networks, 7(2), pp.385-396.

[51] Ruoti, S., Andersen, J. and Seamons, K., 2016, June. Strengthening Password-based Authentication. In Symposium on Usable Privacy and Security (SOUPS).

[52] Cheswick, W.R., Bellovin, S.M. and Rubin, A.D., 2003. Firewalls and Internet security: repelling the wily hacker. Addison-Wesley Longman Publishing Co., Inc.

[53] Herley, C. and Van Oorschot, P., 2012. A research agenda acknowledging the persistence of passwords. IEEE Security & Privacy, 10(1), pp.28-36.

[54] Yahoo (2012). Yahoo says it's investigating security breach. [online] (July 12, 2012). http://www.bloomberg.com/news/2012-07-12/yahoospokeswoman-says-company-investigating-security-breach.html.(Accessed September 15, 2014)

[55] Schneier, B. (2006) MySpace passwords aren't so dumb [online] (Dec. 14, 2006).

http://www.wired.com/politics/security/commentary/securitymatters/2006/12/72300. (Accessed January 15, 2015)

[56] Shay, R., Komanduri, S., Kelley, P.G., Leon, P.G., Mazurek, M.L., Bauer, L., Christin, N. and Cranor, L.F., 2010, July. Encountering stronger password requirements: user attitudes and behaviors. In Proceedings of the Sixth Symposium on Usable Privacy and Security (p. 2). ACM.

[57] Egelman, S., Sotirakopoulos, A., Muslukhov, I., Beznosov, K. and Herley, C., 2013, April. Does my password go up to eleven? the impact of password meters on password selection. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 2379-2388). ACM

[58] Van Acker, S., Hausknecht, D., Joosen, W. and Sabelfeld, A., 2015, March. Password meters and generators on the web: From large-scale empirical study to getting it right. In Proceedings of the 5th ACM Conference on Data and Application Security and Privacy (pp. 253-262). ACM.

[59] Vossaert, J., Lapon, J. and Naessens, V., 2014. Out-of-Band Password Based Authentication towards Web Services. In ECUMICT 2014 (pp. 181-191). Springer International Publishing.

[60] Teh, P.S., Teoh, A.B.J. and Yue, S., 2013. A survey of keystroke dynamics biometrics. The Scientific World Journal, 2013.

[61] Villatte, N. (2015) Data Breach Investigations Report, Verizon RISK Team [online] www.verizonenterprise.com/ DBIR/2015/ (Accessed Jan 2016)

[62] Ganesan, Rajesh. "Stepping up security with password management control." Network Security 2016.2 (2016): 18-19.

[63] Villarrubia, C., Fernandez-Medina, E. and Piattini, M., 2006, April. Quality of password management policy. In Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on (pp. 7-pp). IEEE.

[64] Ruffo, G. and Bergadano, F., 2005, September. Enfilter: a password enforcement and filter tool based on pattern recognition techniques. In International Conference on Image Analysis and Processing (pp. 75-82). Springer Berlin Heidelberg.

[65] Smith, S.L., 1987. Authenticating users by word association. Computers & Security, 6(6), pp.464-470.

[66] Schoen, S., Hofmann, M. and Reynolds, R., 2011. Defending Privacy at the US Border.

[67] Das, A., Bonneau, J., Caesar, M., Borisov, N. and Wang, X., 2014, February. The Tangled Web of Password Reuse. In NDSS (Vol. 14, pp. 23-26).

[68] Weir, M., Aggarwal, S., Collins, M. and Stern, H., 2010, October. Testing metrics for password creation policies by attacking large sets of revealed passwords. In Proceedings of the 17th ACM conference on Computer and communications security (pp. 162-175). ACM.

[69] Yan, J., Blackwell, A., Anderson, R. and Grant, A., (2000). The memorability and security of passwords–some empirical results [online] Technical report (No. UCAM-CL-TR-500). University of Cambridge, Computer Laboratory. http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-500.pdf (Accessed January 15, 2016).

[70] Taha, M.M., Alhaj, T.A., Moktar, A.E., Salim, A.H. and Abdullah, S.M., 2013, August. On password strength measurements: Password entropy and password quality. In Computing, Electrical and Electronics Engineering (ICCEEE), 2013 International Conference on (pp. 497-501). IEEE.

[71] Yan, J.J., 2001, September. A note on proactive password checking. In Proceedings of the 2001 workshop on New security paradigms (pp. 127-135). ACM.

[72] Menezes, A.J., Van Oorschot, P.C. and Vanstone, S.A., 1996. Handbook of applied cryptography. CRC press.

[73] Gong, L., Lomas, M.A., Needham, R.M. and Saltzer, J.H., 1993. Protecting poorly chosen secrets from guessing attacks. IEEE journal on Selected Areas in Communications, 11(5), pp.648-656.

[74] Kehne, A., Schönwälder, J. and Langendörfer, H., 1992. A nonce-based protocol for multiple authentications. ACM SIGOPS Operating Systems Review, 26(4), pp.84-89.

[75] Neuman, B.C. and Stubblebine, S.G., 1993. A note on the use of timestamps as nonces. ACM SIGOPS Operating Systems Review, 27(2), pp.10-14.

[76] Syverson, P., 1993. On key distribution protocols for repeated authentication. ACM SIGOPS Operating Systems Review, 27(4), pp.24-30.

[77] Watro, R., Kong, D., Cuti, S.F., Gardiner, C., Lynn, C. and Kruus, P., 2004, October. TinyPK: securing sensor networks with public key technology. In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (pp. 59-64). ACM.

[78] Xu, J., Zhu, W.T. and Feng, D.G., 2009. An improved smart card based password authentication scheme with provable security. Computer Standards & Interfaces, 31(4), pp.723-728.

[79] Song, R., 2010. Advanced smart card based password authentication protocol. Computer Standards & Interfaces, 32(5), pp. 321-325.

[80] Yang, F.Y., Hsu, C.W. and Chiu, S.H., 2014, January. Password authentication scheme preserving identity privacy. In Measuring Technology and Mechatronics Automation (ICMTMA), 2014 Sixth International Conference on (pp. 443-447). IEEE.

[81] Garrett, K., Talluri, S.R. and Roy, S., 2015. On vulnerability analysis of several password authentication protocols. Innovations in Systems and Software Engineering, 11(3), pp.167-176.

[82] Peyravian, M. and Zunic, N., 2000. Methods for protecting password transmission. Computers & Security, 19(5), pp.466-469

[83] Hwang, J.J. and Tzu-Chang, Y.E.H., 2002. Improvement on Peyravian-Zunic's password authentication schemes. IEICE Transactions on Communications, 85(4), pp.823-825.

[84] Wong, K.H., Zheng, Y., Cao, J. and Wang, S., 2006, June. A dynamic user authentication scheme for wireless sensor networks. In Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference on (Vol. 1, pp. 8-pp). IEEE.

[85] Das, M.L., 2009. Two-factor user authentication in wireless sensor networks. IEEE Transactions on Wireless Communications, 8(3), pp.1086-1090.

[86] Li, C.T. and Lee, C.C., 2012. A novel user authentication and privacy preserving scheme with smart cards for wireless communications. Mathematical and Computer Modelling, 55(1), pp.35-44.

[87] Jiang, Q., Ma, J., Li, G. and Ma, Z., 2013. An improved password-based remote user authentication protocol without smart cards. Information Technology and Control, 42(2), pp.113-123.

[88] Shamir, A., 1984, August. Identity-based cryptosystems

and signature schemes. In Workshop on the Theory and Application of Cryptographic Techniques (pp. 47-53). Springer Berlin Heidelberg.
[89] Shiuh-Jeng, W. and Jin-Fu, C., 1996. Smart card based secure password authentication scheme. Computers & Security, 15(3), pp.231-237.
[90] Jarecki, S., Krawczyk, H., Shirvanian, M. and Saxena, N., 2016, May. Device-enhanced password protocols with optimal online-offline protection. In Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security (pp. 177-188). ACM.
[91] Petsas, T., Tsirantonakis, G., Athanasopoulos, E. and Ioannidis, S., 2015, April. Two-factor authentication: is the world ready? quantifying 2FA adoption. In Proceedings of the Eighth European Workshop on System Security (p. 4). ACM.
[92] Jablon, D.P., 1996. Strong password-only authenticated key exchange. ACM SIGCOMM Computer Communication Review, 26(5), pp.5-26.
[93] Katz, J., Ostrovsky, R. and Yung, M., 2002, September. Forward secrecy in password-only key exchange protocols. In International Conference on Security in Communication Networks (pp. 29-44). Springer Berlin Heidelberg.
[94] Yang, W.H. and Shieh, S.P., 1999. Password authentication schemes with smart cards. Computers & Security, 18(8), pp.727-733.
[95] Abdalla, M., Benhamouda, F. and Pointcheval, D., 2017, March. Removing erasures with explainable hash proof systems. In IACR International Workshop on Public Key Cryptography (pp. 151-174). Springer, Berlin, Heidelberg.
[96] Gennaro, R., 2008, March. Faster and shorter password-authenticated key exchange. In Theory of Cryptography Conference (pp. 589-606). Springer Berlin Heidelberg.
[97] Benhamouda, F., Blazy, O., Chevalier, C., Pointcheval, D. and Vergnaud, D., 2013. New techniques for SPHFs and efficient one-round PAKE protocols. In Advances in Cryptology–CRYPTO2013 (pp. 449-475). Springer Berlin Heidelberg.
[98] Manulis, M., Stebila, D., Kiefer, F. and Denham, N., 2016. Secure modular password authentication for the web using channel bindings. International Journal of Information Security, 15(6), pp.597-620.
[99] Abdalla, M., Chevassut, O., Fouque, P.A. and Pointcheval, D., 2005, December. A simple threshold authenticated key exchange from short secrets. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 566-584). Springer, Berlin, Heidelberg.
[100] Tsai, H.C. and Chang, C.C., 2013. Provably secure three party encrypted key exchange scheme with explicit authentication. Information Sciences, 238, pp.242-249.
[101] Yoneyama, K., 2008, December. Efficient and strongly secure password-based server aided key exchange. In International Conference on Cryptology in India (pp. 172-184). Springer Berlin Heidelberg.
[102] Boyen, X., 2009, March. Hidden credential retrieval from a reusable password. In Proceedings of the 4th International Symposium on Information, Computer, and Communications Security (pp. 228-238). ACM.
[103] Ford, W. and Kaliski, B.S., 2000. Server-assisted generation of a strong secret from a password. In Enabling Technologies: Infrastructure for Collaborative Enterprises, 2000. (WET ICE 2000). Proeedings. IEEE 9th International Workshops on (pp. 176-180). IEEE.
[104] Bagherzandi, A., Jarecki, S., Saxena, N. and Lu, Y., 2011, October. Password-protected secret sharing. In Proceedings of the 18th ACM conference on Computer and Communications Security (pp. 433-444). ACM.
[105] Messerges, T.S., Dabbish, E.A. and Sloan, R.H., 2002. Examining smart-card security under the threat of power analysis attacks. IEEE transactions on computers, 51(5), pp.541-552.
[106] Jaspher, G., Katherine, W., Kirubakaran, E. and Prakash, P., 2012, July. Smart card based remote user authentication schemes—survey. In Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on (pp. 1-5). IEEE.
[107] Yang, C.C., Wang, R.C. and Chang, T.Y., 2005. An improvement of the Yang-Shieh password authentication schemes. Applied Mathematics and Computation, 162(3), pp.1391-1396.
[108] Sun, D.Z., Huai, J.P., Sun, J.Z. and Li, J.X., 2009. Cryptanalysis of a mutual authentication scheme based on nonce and smart cards. Computer Communications, 32(6), pp.1015-1017.
[109] Liu, J.Y., Zhou, A.M. and Gao, M.X., 2008. A new mutual authentication scheme based on nonce and smart cards. Computer Communications, 31(10), pp.2205-2209.
[110] Hwang, M.S. and Li, L.H., 2000. A new remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics, 46(1), pp.28-30.
[111] Diffie, W. and Hellman, M., 1976. New directions in cryptography. IEEE transactions on Information Theory, 22(6), pp.644-654.
[112] Wang, Y.Y., Liu, J.Y., Xiao, F.X. and Dan, J., 2009. A more efficient and secure dynamic ID-based remote user authentication scheme. Computer communications, 32(4), pp.583-585.
[113] Halderman, J.A., Waters, B. and Felten, E.W., 2005, May. A convenient method for securely managing passwords. In Proceedings of the 14th international conference on World Wide Web (pp. 471-479). ACM.
[114] Syed Zulkarnain Syed Idrus, Estelle Cherrier, Christophe Rosenberger, Jean-Jacques Schwartzmann. A Review on Authentication Methods. Australian Journal of Basic and Applied Sciences, 2013, 7 (5), pp.95-107. <hal-00912435>.
[115] Czeskis, A., Dietz, M., Kohno, T., Wallach, D. and Balfanz, D., 2012, October. Strengthening user authentication through opportunistic cryptographic identity assertions. In Proceedings of the 2012 ACM conference on Computer and communications security (pp. 404-414). ACM.

Authors' Profiles

Amanpreet Kaur received her MCA. Degree from GGSIP University, India in 2009 and currently pursuing her Ph.D. degree in Computer Science, at Jamia Millia Islamia. She has been working as an Assistant Professor in SGTBIMIT College affiliated to GGSIP University from last 8 years. Her research interests include Information Security, Authentication, Cryptography, software security, Identity management and Security policies and standards.

Prof Khurram Mustafa (b.1964), graduated first with a masters' degree in 'Mathematics with Computer Science' from Jamia Millia Islamia, New Delhi; followed by MTech & PhD, from IIT Delhi, India. Though, he did his PhD on an interdisciplinary topic related to eLearning, he continues to supervise/write/speak on diverse fields pertaining to eLearning, information security and Research Methods in Computer Science. He is currently working as a Professor of Computer Science. During his prolonged career of over two decades, he has the distinction of being the founder Head of the department in year 2000 and establishing the same during his 3 tenures as HoD. 5 years' tenure, as a professor and an Associate professor. He has supervised more than a dozen PhD students towards completion, coauthored 2 books (published by Narosa, India and the international edition by Alpha Science, UK), out of those one has been translated to Chinese language. Apart from these on the academic contributions upfront, he has co-authored several book chapters and over 100 research papers, published in international journals and conference proceedings. He also led a 3-years government funded project as PI - in the field of information security and delivered more than 50 invited-talks, including keynote-addresses. In addition, he is on several statuary committees, editorial review boards; and a member of several professional scientific societies in including ISTE, ICST, EAI, ACM-CSTA, eLearning Guild & InfoPier.

How to cite this paper: Amanpreet A. Kaur, Khurram K. Mustafa,"A Critical appraisal on Password based Authentication", International Journal of Computer Network and Information Security(IJCNIS), Vol.11, No.1, pp.47-61, 2019.DOI: 10.5815/ijcnis.2019.01.05

