Passwords and the Evaluation of Imperfect Authentication Schemes

Aasminpreet Singh Kainth
Department of Computer Science
Middlesex College, University of Western Ontario
London, Ontario, Canada.
akainth4@uwo.ca

Abstract - Identity verification is the key to the platform economy, and it can even be said to be the pillar of the fourth industrial revolution. From machines that require authentication to Internet of Things (IoT) devices that communicate with machines, to A.I and blockchain that will be used to protect and bypass the authentication system, trustworthy authentication is the key. Its verification relies heavily on passwords. Thus, I evaluated a few promising proposals to replace text passwords using fifteen usability and security factors that an ideal authentication scheme might provide. Beyond the analysis of current schemes, the mentioned factors can be used to evaluate any future authentication proposal. [1]

I. Introduction

A. Problem Formulation

Using passwords [1] will force users to create and store complex mixtures of letters, numbers, symbols, and upper and lower case; change passwords frequently; and try to avoid reusing passwords between accounts. Users often manage at least 20 passwords, and the information and tools they need to manage are exploding. To log in to digital tools simply and effectively, users are facing increasing challenges, so they tend to reuse the same password.

Passwords are indeed [1]at the core of the data breach problem. According to the data breach investigation report released by Verizon in 2019, 80% of hacker-related data breaches are related to weak passwords, and 29% [1] of all data breaches involve the use of stolen passwords. This kind of attack has promoted the booming development of the underground economy, which has further exacerbated the problem of data leakage.

As companies increasingly drive business valuations and business growth on platform businesses, digital trust issues are also growing rapidly and [1] damaging the confidence of entire online communities. Individuals are cautious about providing too much personal information; partners are worried about losing confidential information and business processes; when systems and customers are damaged, global companies will bear the risk of reputation and revenue damage.

Identity verification must be an integral part of the user experience. This is not only a question answered with technology, it is also related to the idea of system design. User experience has become a strong competitive advantage and the main driving force for the transition to passwordless technology [2]. Identity authentication should be designed as a whole, using open standards to ensure internal and external interoperability of the company, and based on adaptability, security and privacy awareness, build user trust, better service, and successfully pass time test.

B. Motivation

Although it is essential to develop a long-term authentication strategy, [1] believe that the next digital breakthrough will be passwordless authentication, mainly for security reasons, but the reasons are not limited to this.

Compared with traditional personal information-based authentication (KBA), passwordless authentication has four key advantages [1]. First, passwordless authentication is economically meaningful: it increases revenue and reduces costs. Secondly, from the customer's perspective, this verification method is meaningful because it provides a better user experience. Third, from a strategic point of view, it can help redefine competition by unlocking value from interoperability. Fourth, as already mentioned, it greatly improves security.

To accomplish this goal, the following tasks are set:

(i) finding new authentication scheme proposals to replace passwords

(ii) identifying the criteria on which these authentication schemes should be jointly compared

(iii) comparing schemes on identified criteria

The rest of the paper is organized as follows. Section 2 provides the background information of the papers read. Section 3 outlines the evaluation criteria proposed. The discussion to research is presented in Section 4, while Section 5 aims to conclude. Section 6 gives references to research papers discussed.

II. LITERATURE REVIEW

There are many techniques to replace passwords. Each of these technologies has advantages and disadvantages, depending on the organization's own environment, original systems, and goals that use them.

A. Encrypted Password managers

a. Google Chrome (Browser based)

[3] being the most popular password manager stores the passwords online which makes the password access available to all devices connected online. Google Password Manager does all the entry-level jobs of a traditional password manager, i.e., saving passwords and autofill info. But the best thing about this free tool of Google is the ease of work it offers. You're not required to download any app or browser extension or even create an additional account for it.

A Google account (which all of us have) and Google Chrome browser (again, which all of us use) are enough to get you up and running.

b. Lastpass (Computer based)

[4] is a password manager for all platforms (from mobile phones to various browsers). You only need to remember the account password of LastPass itself, and the account passwords of other websites, all will be encrypted and saved to the cloud by LastPass. In this way, you no longer waste energy and brainpower to record the account passwords of other websites. This kind of trivial matter can be handled by LastPass.

The password in [4] is protected by a master password, encrypted locally, and can be synchronized to any browser. LastPass also supports automatic form filling, random password generation and password sharing. LastPass provides a variety of cross-platform browser plug-ins, which can provide secure and convenient password management and automatic form filling functions for these browsers, replacing the insecure browser itself Password manager.

B. Graphical centered systems

a. Persuasive Cued Click-Points:

In [5] a novel recognition-based and recall-based graphical password creation is proposed which is based on the memorability of graphical password. In the First authentication set up phase, user are given a set of 25 images to select from where after selecting some images, system asks 3 questions to user for which one has to select regions of answer in the images selected. In the second step, the system employs cued recalled-based methods which randomizes the question number in some three digit format which makes it harder for any bystander to retain the relationship between questions and the points. Apparently, the hurdles of the system includes the screen capturing application.

b. Passfaces:

[6] showed up with implicit password authentication framework by engaging a graphical password and text-based authentication. This framework uses users' database images where each image will have at least one clickable point to which some information associated. Here, framework expects users to store ample amount of information related to predefined topics where the system would then analyse, extract and relate this information using intelligent image server built by admin. Authentication is pretty much similar to the one defined in *Persuasive Cued Click-Points*. Major advantages add up the prevention of shoulder surfing also replay attacks or sniffing exchanged information appears useless to attackers. If the attackers knows the victim very well or if attacker is able to gather information by checking the victims profile then he can fool the system and can take access. In order to make the framework more secure, it is suggested to have tons of images and resources to avoid short cycle repetition which requires human interaction to add clickable objects and text attributes to those objects within the picture.

c. Image PassCode (IPCT):

[7] proposed a new mobile based authentication system which applies image PassCode with a tapping scheme, named IPCT. It consisted of an accelerometer, selection of n images, tapping fingers and the time duration of holding buttons in order to provide a more reliable method of authentication. It can be indicated from the comparison that IPCT has the highest level of dependability and lowest complexity on memorability.

C. *Cognitive authentication*

a. GrIDsure

GrIDsure [8] is a flexible authentication method that provide the end-user with a matrix of cells which consists of random characters, from which one has to choose a 'personal identification pattern' (PIP).
Whenever a user wants to authenticate to a protected resource, they are assigned with a challenge grid consisting of random characters. The user then enters the characters in the cells which correspond to their PIP.
This scheme resembles passwords in terms of usability and perhaps rate it is identically in terms of many usability assistance.

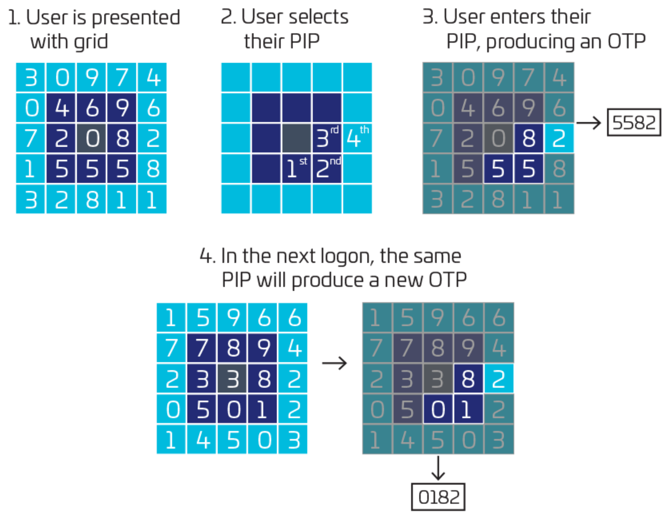
1. User is presented with grid
30974
04696
72082
15558
32811
2. User selects their PIP
3rd
4th
1st
2nd
3. User enters their PIP, producing an OTP
5582
4. In the next logon, the same PIP will produce a new OTP
15966
77894
23382
05012
14503
0182

Figure 1 Grid Authentication [9]

D. Hardware Tokens

a. RSA SecurID:

Hardware tokens are known for storing secrets in a dedicated tamper-resistant module carried by the user [10]. A simple implementation of this device consists only of a display and no buttons or I/O ports. Each instance of the device holds a secret "seed" known to the back-end. A cryptographically strong transform creates a new 6-digit code from this secret every 60 seconds which is presented on the device's display. During the sign up process, user gets connected to back-end via web where he selects a 4-digit PIN and the pairing between username and token is confirmed. To sign in user types the username and concatenated 4-digit pin and dynamic 6-digit code. Adding on, RSA [11] offers a single sign-on facility to grant access to various corporate resources with the same token.

b. YubiKey:

Yubico [12] modeled a USB flash drive namely YubiKey which produces one-time codes. Instead of display, it simulates a USB keyboard, which saves the user from having to transcribe the code, as it prompts user to press the button on YubiKey which types the password. The company recently announced a model which supports the RFID/NFC contactless technology i.e., MIFARE protocol which can be used as a tap-in authentication in smartphones.

E. Smartphone centered

a. Pixie:

[13] replaced the common ways of using a camera in two factor authentication solution for mobile and wearable devices. In Pixie, a user has to capture a unique object caller trinket to get authentication success where the captured picture will be compared to the original picture. If both match together, the user can login in to the smartphone. Just like setting a password, the user picks a readily accessible trinket of her preference, e.g., a clothing accessory, a book, or a desk-toy, then uses the device camera to snap trinket images (a.k.a., reference images). All the user needs to do to authenticate is to point the camera to the trinket.

b. 2FA through near field communication:

[14] presented a two-factor authentication based on NFC smartphone devices. The system is amalgamation of two models, what you have and what you know. Firstly it requires users to enter a passcode which would then unlock the protection of the key on their mobile phones. Then, the key is relocated through NFC to accomplish the login process. Although the privacy and protection of the key store leaves android OS sandboxing, there is no other second solution in order to defy zero-day vulnerabilities.

c. Multipurpose speech watermarking:

[15]created a multi-factor authentication scheme based on speech, PIN code and OTP [16] which were combined up in generating a reliable watermarking. The blending of the biometric of the user along with PIN code with applying a key to generate a hash to use in watermarking technique; does not let the password crackers to run brute force attack simply. By concealing the PIN code and the OTP within speech signals, they considered that it is hard to Eavesdrop or steal these items. Also, the specificity of the OTP as a time-stamp can stop session hijacking threats.

d. Google 2-Step:

Introduced in 2011, Google 2-Step Verification [17] is a commercial offering that combines a user's traditional, memorized password with one-time codes, which are either sent over SMS or voice to a registered phone or can be generated as time-dependent passwords by a dedicated mobile phone application called The scheme also supports long, printable backup secrets for override in the case of a lost phone.

F. Web centered systems [18]

a. Web Transaction Using E-Smart Cards:

[19] contemplated a two-factor authentication system for safeguarding the privacy of transactions in a web-based environment. Their proposed method consisted of an image and a smart card to clear the authentication process. A smart card reader is required in reading the parameters stored in a smart card. Also, the user must submit username and password. To prevent the replay attack, time is among one of the parameters that has to be sent. Image is also required from which master key is extracted. After this, to compare the equality of the master key, it is sent to the server which performs the same calculations and on the same image. As per the analysis, more the number of users, more would be the communication and computational cost on the server side.

b. Biometric Behavioral authentication:

[20] proposed a robust way for identifying users through a biometric behavioural authentication system which combines keyboard dynamics, GUI and mouse interactions data. The main aim of this type of application was to collect information related to key press, mouse moves, releases, mouse clicks and program window's controls by retrieving windows hooking chain. After extracting features, each part is understood by a different algorithm. As

per their experimental results, BayesNet classifier was the one of the best among other algorithms with the identification accuracy of 99.39%. This result bolsters the idea of merging different modalities for gaining better consequences Moreover, keystroke features were finest among other two approaches.

G. EEG-based centered systems

a. Biometric EEG authentication:

[21] shed light on future authentication system via EEG devices providing a secure two factor authentication though the device is not easily accessible for everyone right now. The author used Electroencephalography ~ *uh·lek·trow·uhn·seh·fuh·laa·gruh·fee* sensor for the creation of password where a password is chopped into smaller snips and, for each snip mental state comes into play to provide verification. Pros of this scheme is the signal cannot be recreated and con being the computer infected with malware can capture signals. Threats like replay attack or shoulder surfing are mitigated as the system more secure with the mixture of brain signals and password. [22] achieved better results by combining brain waves and eye blinking Electro-Oculo-Gram (EOG) artifacts to create a robust scheme for *biometric EEG authentication*.

b. Pass-Thought :

[23] proposed a Brain-computer interface system, designed to gather signals from brain-waves based on a thought to identify each person’s identity. Pass-thoughts works by highlighting elements of a textual or graphical password accidentally and capturing signals produced by the sensor (yes/no). Downside of this system is that phishing is still a successful attack against this system. The requirement of additional hardware is also controversial, but definitely, it could be used for specific purposes and organizations where security is a vital and high-valued element.

H. Biometrics [24]

a. Fingerprint recognition:

[25] The Fingerprint recognition process is divided into two parts: user registration and feature matching. [26] Whether it is the verification or identification process, the fingerprint image of the user to be identified needs to be subjected to a series of steps such as image segmentation, refinement, binarization, feature extraction, etc., to generate the same data format as the database template, and finally, compare and get the recognition result.

b. Iris recognition:

[27] Iris recognition technology is the application of computer to quantitative data analysis of iris pattern features to confirm the true identity of the recognized person. In the recognition process, the face of the incoming person is captured through the infrared camera, then the iris is located and the features are extracted for calculation, and then compared with the inventory data in the database , and finally judged and taken measures.

Retinal scanning [25] uses laser light to irradiate the back of the eyeball, scans and captures hundreds of characteristic points of the retina, and forms a memory template after digital processing and stores it in the database for later comparison and verification. The retina is an extremely stable biological feature, and it is a highly accurate identification technology as identity authentication.

c. Voice recognition:

[28] Voice recognition, also commonly referred to a voiceprint, is a kind of behavior recognition technology. The voice recognition equipment continuously measures and records the waveform and changes of the sound, and performs spectrum analysis. After digital processing, it is made into a sound template and stored. When using, the sound collected on the spot is registered with The sound template is accurately matched to identify the person’s identity. This technology has poor accuracy and is difficult to use, and is not suitable for direct digital signatures and network transmission. Voice recognition is a technology that recognizes by analyzing the physical characteristics of the user's voice [29]

d. [30] Ultrasonic Fingerprint:

To actually capture the details of a fingerprint, the hardware consists of both an ultrasonic transmitter and a receiver. An ultrasonic pulse is transmitted against the finger that is placed over the scanner. Some of this pulse is absorbed and some of it is bounced back to the sensor, depending upon the ridges, pores and other details that are unique to each fingerprint. The 3D nature of this capture technique makes it an even more secure alternative to capacitive scanners.

III. Evaluation Criteria

Security technology often has a short cycle and develops rapidly. Whether operating for a year or a decade or more, cybercriminals are usually good at finding ways to circumvent security controls. Identity verification technology is no exception. Therefore, it is essential to develop a long-term security strategy.

Although the "privacy issue" authentication method should have long been abandoned, and passwordless authentication is the future development direction, but when constructing an authentication program that can pass the test of time, following principles should be considered:

A. Security & Stability

When formulating an authentication system strategy, logically security is the first. The security of the authentication system will be based on a variety of considerations, from the formation of relative advantages compared with other solutions, to the lifetime of new threats faced by known threats and systems, as well as the hardware and software vulnerabilities that it solves and introduces.

The security of the identity verification system also depends on its efficiency in reducing fraud and risks, as well as its reliability through logging.

S1. *Resilient-to-Physical-Observation*: An attacker cannot impersonate a user after observing them authenticate one or more times. Attacks include shoulder surfing, filming the keyboard, recording keystroke sounds, or thermal imaging of keypad.

S2. Resilient-to-Targeted-Impersonation: It is not possible for an acquaintance to impersonate a specific user by exploiting knowledge of personal. Personal knowledge questions are the canonical scheme that fails on this point.

S3. Resilient-to-Throttled-Guessing: An attacker whose rate of guessing is constrained by the verifier cannot successfully guess the secrets of a significant fraction of users.

S4. Resilient-to-Unthrottled-Guessing: An attacker whose rate of guessing is constrained only by available computing resources cannot successfully guess the secrets of a significant fraction of users. Lack of this benefit is meant to penalize schemes where the space of credentials is not large enough to withstand brute force search *(including dictionary attacks, rainbow tables and related brute force methods smarter than raw exhaustive search, if credentials are user-chosen secrets).*

S5. Resilient-to-Internal-Observation: An attacker cannot impersonate a user by intercepting the user's input from inside the user's device (e.g., by key-logging malware) or eavesdropping on the cleartext communication between prover and verifier. This benefit assumes that general-purpose devices like software-updatable personal computers and mobile phones may contain malware, but that hardware devices dedicated exclusively to the scheme can be made malware-free.

S6. Resilient-to-Phishing: An attacker who simulates a valid verifier (including by DNS manipulation) cannot collect credentials that can later be used to impersonate the user to the actual verifier. This penalizes schemes allowing phishers to get victims to authenticate to lookalike sites and later use the harvested credentials against the genuine sites.

S7. Resilient-to-Theft: If the scheme uses a physical object for authentication, the object cannot be used for authentication by another person who gains possession of it.

S8. Requiring-Explicit-Consent: The authentication process cannot be started without the explicit consent of the user. This is both a security and a privacy feature (a rogue wireless RFID-based credit card reader embedded in a sofa might charge a card without user knowledge or consent).

B. Usability & User Adoption

User experience is no longer an optional, better choice, it has become a key differentiating factor: the quality of user experience determines user choices, preferences and behaviors. Therefore, future identity verification should strive to provide a seamless user experience to ensure applicability.

The platform economy requires large-scale solutions. Employees and end users will increasingly cross different platforms for identity verification. Therefore, it is important to consider identity verification solutions from the perspective of scale: the platform reaches a critical mass and begins to produce network effects, and the growth may be exponential. The performance goals of the certification system need to be planned long in advance, especially around reliability and availability.

U1. Memorywise-Effortless: Users of the scheme do not have to remember any secrets at all.

U2. Nothing-to-Carry: Users do not need to carry an additional physical object (electronic device, mechanical key, piece of paper) to use the scheme. Exception if the object is one that they'd carry everywhere all the time anyway, such as their mobile phone, but not if it's their computer (including tablets).

U3. Physically-Effortless: The authentication process does not require physical (as opposed to cognitive) user effort beyond, say, pressing a button. Schemes that don't offer this benefit include those that require typing, scribbling or performing a set of motions. Exception if the user's effort is limited to speaking, on the basis that even illiterate people find that natural to do.

U4. Easy-to-Learn: Users who don't know the scheme can figure it out and learn it without too much trouble, and then easily recall how to use it.

U5. Efficient-to-Use: The time the user must spend for each authentication is acceptably short. The time required for setting up a new association with a verifier, although possibly longer than that for authentication, is also reasonable.

U6. Infrequent-Errors: The task that users must perform to log in usually succeeds when performed by a legitimate and honest user. In other words, the scheme isn't so hard to use or unreliable that genuine users are routinely rejected.

U7. Easy-Recovery-from-Loss: A user can conveniently regain the ability to authenticate if the token is lost or the credentials forgotten. This combines usability aspects such as: low latency before restored ability; low user inconvenience in recovery (e.g., no requirement for physically standing in line); and assurance that recovery will be possible, for example via built-in backups or secondary recovery schemes. If recovery requires some form of re-enrollment, this benefit rates its convenience.

IV. Discussion

A clear result to the review of all the authentication methods considered states that not a single authentication scheme is perfect. Each scheme has its own strengths and weaknesses. Such as EEG based schemes perform better than the traditional password scheme in security measures but in terms of ease of usability it depicts a complete red i.e. perform worse than the traditional password authentication scheme. Table 1 depicts the comparative evaluation of the various schemes examined across the literature review. The most significant worthy note which can be obtained from the table is that all authentication schemes do better than the traditional passwords in some way, but it is also vivid that all are worse than the others as no row is free of red (horizontal) stripe. Some of the schemes have so solid secure approach but they might be hard to implement and complicated to use as there might be people who are not so familiar with the computer technologies. Each client has different learning, memorability and knowledge capability which makes it difficult to produce a perfect or close to perfect authentication scheme. Hence, the quest to replace traditional passwords seems dull as per current available technologies.

		Security								Usability						
Category	**Scheme**	*Resilient-to-Physical-Observation*	*Resilient-to-Targeted-Impersonation*	*Resilient-to-Throttled-Guessing*	*Resilient-to-Unthrottled-Guessing*	*Resilient-to-Internal-Observation*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*Requiring-Explicit-Consent*	*Memorywise-Effortless*	*Nothing-to-Carry*	*Physically-Effortless*	*Easy-to-Learn*	*Efficient-to-Use*	*Infrequent-Errors*	*Easy-Recovery-from-Loss*
Incumbent	Web Passwords	⬛	🟨	⬛	⬛	⬛	⬛	🟨	🟨	🟨	🟨	⬛	🟨	🟨	🟨	🟨
Password Managers	Chrome (Browser based)	⬛	🟨	🟨	⬛	🟨	🟩	🟨	🟨	🟨	🟥	🟩	🟨	🟨	🟨	🟥
	LastPass (Computer based)	⬛	🟨	🟩	🟩	🟨	🟩	🟨	🟨	🟨	🟥	🟩	🟨	🟨	🟨	🟥
Graphical	Persuasive Cued Click-Points	⬛	🟩	🟩	⬛	🟨	🟩	🟨	🟨	🟥	🟨	🟥	🟨	🟥	🟥	🟨
	PassFaces (Locimetric Scheme)	⬛	🟩	⬛	⬛	🟨	⬛	🟨	🟨	🟥	🟨	🟥	🟨	🟥	🟥	🟨
Cognitive	GrIDsure	⬛	🟩	⬛	⬛	🟨	⬛	🟨	🟨	🟥	🟨	🟥	🟨	🟥	🟨	🟨
Hardware Tokens	RSA SecurID	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟨	🟥	🟥	🟨	🟥	🟨	🟥
	Microsoft's YubiKey	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟨	🟥	🟥	🟨	🟥	🟨	🟥
Smart Phone Based	Pixie	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟨	🟥	🟥	🟨	🟥	🟨	🟥
	2FA through near field communication	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟨	🟥	🟥	🟨	🟥	🟨	🟥
	Multipurpose speech watermarking	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟨	🟩	🟥	🟥	🟨	🟥	🟥	🟥
	Google 2-Step	🟩	🟨	🟩	🟩	🟨	🟩	🟨	🟨	🟨	🟥	🟥	🟨	🟥	🟨	🟥
Web Centered	Web Transaction Using E-Smart Cards	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟨	🟥	🟥	🟨	🟥	🟨	🟥
	Biometric Behavioral authentication	🟩	🟥	🟩	⬛	🟨	⬛	🟥	🟨	🟩	🟨	🟩	🟨	🟥	🟥	🟥
EEG Based	Biometric EEG authentication	🟩	🟩	🟩	🟩	🟩	🟥	🟩	🟨	🟩	🟥	🟩	🟥	🟥	🟥	⬛
	Pass-Thought	🟩	🟩	🟩	🟩	🟩	🟥	🟩	🟨	🟩	🟥	🟩	🟥	🟥	🟥	⬛
Biomentric	Fingerprint Recognition	🟩	🟥	🟩	⬛	⬛	🟨	🟥	⬛	🟩	🟨	🟩	🟨	🟥	🟩	🟥
	Iris Recognition	🟩	🟥	🟩	⬛	⬛	🟨	🟥	⬛	🟩	🟨	🟩	🟨	🟥	🟩	🟥
	Voice Recognition	🟩	🟥	🟩	⬛	⬛	🟨	🟥	⬛	🟩	🟨	🟩	🟨	🟥	🟩	🟥
	Ultrasonic fingerprint ID	🟩	🟥	🟩	⬛	⬛	🟨	🟥	⬛	🟩	🟨	🟩	🟨	🟥	🟩	🟥

🟩 = Better than Passwords
🟥 = Worse than Passwords
⬛ = Doesn't offer the benefit/ Can't say

Table 1 COMPARATIVE EVALUATION OF THE VARIOUS SCHEMES EXAMINED

It is observed that password-based schemes such as One-Time passwords, Pin code and ordinary passwords are the most popular choice in most two-factor or multi-factor authentication schemes reviewed. Graphical based authentication schemes are the second most used schemes which are easy to remember and easy to utilize. The fewest number of usages are related to smart-cards, speech recognition, and EEGs , these could have different reasons. For an instance EEGs are hard to carry around for authentication as current EEG sensor technologies are not compact. [31]

Hardware tokens provide better security than the traditional passwords but they need improvement in the usability benefits where the traditional passwords outshine – namely *Easy-Recovery-From-Loss*, *Nothing-to-Carry* and *Physically-Effortless*. None of the token scheme achieves two of these three above mentioned usability benefit. Some pairs of benefits are almost incompatible to each other as in the case of the pair (*Memorywise-Effortless*, *Nothing-to-Carry*) which is only achieve by biometric systems.

a) Rating categories of schemes

Password managers offer nearly the same security and usability benefits. Their major weakness lies in the *recovery from the loss*. One may forget the master password which protects the other passwords, one could lose everything. There are recovery options but none are perfect.

The usability benefits of graphical passwords are a little less than the traditional passwords. Similar is the case with the Cognitive category scheme. Both category schemes hold equivalent security benefits and doesn't hold benefits for the *physical observation.*

The Smart phone based category schemes offer better security benefits than the above mentioned schemes in return of worse usability(e.g., *nor physically-effortless, nor nothing-to-carry, nor efficient-to-use, nor easy-recovery-from-loss*). Evaluation of hardware token schemes and web centered schemes show lean improvement in the security while attempt to give better usability benefits is not a success.

Biometric schemes [24] have similar scores in the usability benefits, and do poorly in security metrics. These are non-resilient to internal observation which is the major concern in this scheme as if malware captures the digital representation of client's fingerprint , possible replay makes the biometric no longer suitable in unsupervised environments. [32] However, biometrics aren't well suited for unsupervised web authentication where client devices lack a trusted input path and means to verify that samples are live. [18]

V. Conclusion

The brief tabulated overview in the table 1 helps us observe the red, green and black patterns depicting the benefits and the comparison to the traditional password that might otherwise be missed. At this point, many conclusions can be made such as Hardware token and EEG based authentication systems appear most secure, but their usability scores are much less than that compared to traditional passwords.

However, each of the authentication category has some issues which make them unreliable. The knowledge based systems are non-resilient to physical observation, Biometric based authentication schemes are prone to advanced threats such as 3D modelling of a face or finger. At the same time, a *recovery-from-the-loss* is a vital matter which increases the complexity of a Hardware token systems. Therefore, some schemes do better and some do worse than the other which still increase the potential to find an alternative to passwords.

VI. References

[1] "Verizon 2020 Data Breach Investigations Report," Verizon, 2019. [Online]. Available: https://enterprise.verizon.com/resources/reports/dbir/.

[2] L. Wang, Y. Li and K. Sun, "Amnesia: A Bilateral Generative Password Manager," June 2016.

[3] "Chrome Password Manager," Google, [Online]. Available: https://support.google.com/chrome/answer/95606?hl=en.

[4] "LastPass," [Online]. Available: https://www.lastpass.com/how-lastpass-works.

[5] A. S. Gokhalea and V. S. Waghmare, "The Shoulder Surfing Resistant Graphical Password Authentication Technique," *Proceedings of International Conference on Communication, Computing and Virtualization (ICCCV) ,* vol. 79, pp. 490-498, 2016.

[6] S. Almuairfi, P. Veeraraghavan and N. Chilamkurti., "A novel image-based implicit password authentication system (IPAS) for mobile and non-mobile devices," *International Symposium on Computational Electronics,* vol. 58, no. 1-2, pp. 108-116, July 2013.

[7] V. Shankara, K. Singha and A. Kumar, "IPCT: A scheme for mobile authentication," *Perspectives in Science,* vol. 8, pp. 522-524, September 2016.

[8] R. Jhawar, P. Inglesant, N. Courtois and M. A. Sasse, "Makemine a quadruple: Strengthening the security of graphical one-time pin authentication," *NSS,* pp. 81-88, 2011.

[9] THALES, "Grid Authentication," [Online]. Available: https://cpl.thalesgroup.com/access-management/authenticators/grid-authentication.

[10] "RSA SecurID Two-factor Authentication," [Online]. Available: www.rsa. com/products/securid/sb/10695_SIDTFA_SB_0210.pdf.

[11] P. Bright, "RSA finally comes clean: SecurID is compromised," June 2011. [Online]. Available: arstechnica.com/security/news/2011/06/ rsa- finally- comes-clean- securid- is- compromised.ars.

[12] "Yubico," Yubico, [Online]. Available: https://www.yubico.com/works-with-yubikey/catalog/microsoft-accounts/.

[13] M. Azimpourkivi, U. Topkara and B. Carbunar, "Camera based two factor authentication through mobile and wearable devices.," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies,* vol. 1, no. 3, September 2017.

[14] M. A. Crossman and H. Liu, "Two-factor authentication through near field communication," *IEEE,* September 2016.

[15] M. A. Nematollahi, H. Gamboa-Rosales, F. J. Martinez-Ruiz, J. I. D. l. Rosa-Vargas, S. A. R. Al-Haddad and M. Esmaeilpour, "Multi-factor authentication model based on multipurpose speech watermarking and online speaker recognition," *https://doi.org/10.1007/s11042-016-3350-1,* March 2017.

[16] D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache and O. Ranen., IETF, RFC 4226, [Online]. Available: https://tools.ietf.org/html/rfc4226.

[17] Google Inc., "2-step verification: how it works," Google Inc., 2012. [Online]. Available: www. google.com/accounts.

[18] F. Alaca, A. M. Abdou and P. V. Oorschot., "Comparative Analysis and Framework Evaluating Mimicry-Resistant and Invisible Web Authentication Schemes," April 2019.

[19] M. N. Ahmed and M. Hussain, "Privacy Preserving Web Based Transaction Using E-Smart Cards and Image Authentication. In: Proceedings," *ICACCE (IEEE International Conference on Advances in Computing and Communication Engineering),* p. 465–470, 2016.

[20] K. O. Bailey, J. S. Okolica and G. L. Peterson, "User identification and authentication using multi-modal behavioral biometrics.," *http://dx. doi.org/10.1016/j.cose.2014.03.005.,* vol. 43, pp. 77-89, June 2014.

[21] I. Švogor and T. Kišasondi, "Two factor authentication using EEG augmented passwords," *Inf. Technol. Interfaces,* p. 373–378, December 2016.

[22] Abo-Zahhad, M. Ahmed, S.M., Abbas and S.N., "A new multi-level approach to EEG based human authentication using eye blinking.," 2015.

[23] J. Thorpe, P. C. v. Oorschot and A. Somayaji, "Pass-thoughts: authenticating with our minds," *NSPW,* p. 45–56, September 2005.

[24] A. K. Jain, A. Ross and S. Pankanti, "Biometrics: a tool for in-formation security," *IEEE Transactions on Information Forensics and Security,* vol. 1, no. 2, pp. 125-143, June 2006.

[25] Wikipedia, "Wikipedia," [Online]. Available: wikipedia.com.

[26] A. Ross, J. Shah and A. K. Jain, "From Template to Image: Reconstructing Fingerprints from Minutiae Points," *IEEE Trans. Pattern Anal. Mach. Intell.,* vol. 29, no. 4, p. 544–560, 2007.

[27] Android Aauthority, "Android Aauthority," [Online]. Available: https://www.androidauthority.com.

[28] find biometrics, "find biometrics," [Online]. Available: findbiometrics.com.

[29] P. S. Aleksic and A. K. Katsaggelos, "Audio-Visual Biometrics," vol. 94, no. 11, p. 2025–2044, 2006.

[30] Samsung, "Samsung patent explores ultrasonic fingerprint," August 2018. [Online]. Available: https://www.planetbiometrics.com/article-details/i/7365/desc/samsung-patent-explores-ultrasonic-fingerprint/.

[31] M. H. Barkadehi, M. Nilashi, O. Ibrahim, A. Z. Fardi and S. Samad., "Authentication systems: A literature review and classification," *Telematics and Informatics,* vol. 35, no. 5, pp. 1491-1511, August 2018.

[32] A. Alhothaily, C. Hu, A. Alrawais, T. Song, X. Cheng and D. Chen., "A Secure and Practical Authentication Scheme Using Personal Devices," *IEEE Access,* vol. 5, pp. 11677 - 11687, June 2017.