Augmented Cognition for Continuous Authentication

Nancy Mogire[1(✉)], Michael-Brian Ogawa[1], Brent Auernheimer[2], and Martha E. Crosby[1]

[1] Department of Information and Computer Sciences,
University of Hawaii at Manoa, Honolulu, HI 96822, USA
{nmogire, ogawam, crosby}@hawaii.edu
[2] Computer Science Department,
California State University, Fresno, CA 93740, USA
brent@csufresno.edu

Abstract. Authentication serves the gatekeeping function in computing systems. Methods used in authentication fall into three major paradigms: 'what you know', 'who you are' and 'what you have' of which the first is still the most commonly applied in the form of passwords authentication. Recall and recognition are the cognitive functions central to the 'what you know' authentication paradigm. Studies have shown that more secure passwords are harder to recall and this often leads to habits that facilitate recollection at the expense of security. Combining the uniqueness of physiological measures, such as brainwave patterns, with memorable augmented passwords shows the promise of providing a secure and memorable authentication process. In this paper, we discuss authentication and related problems and considerations in literature. We then test a password system designed to make use of character property transformations such as color and font to minimize the need for complex passwords while not compromising security. The findings from this study suggest that applying transformations to passwords facilitates memorability. We then discuss a study to combine an augmented password system with physiological measures that can provide a more secure model for continuous authentication.

Keywords: Authentication · Password authentication · Brainwave based authentication · Recall and recognition · Password memory · Physiological measures

1 Introduction

Authentication is one of the considerations central to system design since it serves the gate-keeping function in any given system. Authentication can be defined as the process where one entity acquires evidence of the identity claimed by another entity in a protocol in which both entities are involved. Commonly in consumer computing systems, this protocol is the login process. Authentication methods fall into three different paradigms: who you are, what you have and what you know. Various methods drawn from these different paradigms can be combined to form multi-factor authentication systems. This paper details the weaknesses and trade-offs of each of these

D.D. Schmorrow and C.M. Fidopiastis (Eds.): AC 2017, Part I, LNAI 10284, pp. 342–356, 2017.
DOI: 10.1007/978-3-319-58628-1_27

methods. Password authentication which falls under the ‘what you know’ paradigm is most commonly used perhaps due to the lower cost and ease of implementation. As it is susceptible to various attacks, we discuss some causes and possible solutions including the use of physiological measurements for authentication. Since we may be able to capture physiological data from the recall and recognition of passwords, we designed a study to test the memorability of augmented passwords with the goal of designing a system aimed at mitigating password problems.

Physiological characteristics are harder to impersonate than any other authentication form because they are pre-cognitively controlled. While a lot of physiological functioning is non-observable in the physical dimension, its measurement can be obtained by measuring performance of an individual on carefully designed and predefined tasks that reflect various behavioral and bodily functions. For example, we can detect recognition of a password by observing a P300 brainwave pattern obtained using EEG tools. Our eventual goal is to study how these measures can be reliably combined to distinguish between intended and unintended users.

2 Review of the Literature

This review presents the different paradigms of authentication and then focuses on a the ‘what you know’ model of password-based authentication due to its current dominance in user authentication processes. We review the weaknesses of password authentication and the background problems that lead to these weaknesses. Specifically, we focus on recall and recognition and the attempts that have been made at improving these cognitive processes for the sake of password security. Subsequently we review literature on the workings of the brain as underlies cognition. We then introduce brain computer interaction and review studies that have considered the use of brain data for authentication in the way that passwords are used today. Next, we review security propositions in physiological measurement based authentication and finally we look at some security threats resulting from these physiological measurement methods and the potential effectiveness of attacks to these systems. We close this section by reviewing literature on continuous authentication itself a concept that is still relatively new, and its connection to the brainwave based authentication.

2.1 Authentication

Different methods of authentication are susceptible to different attacks. Thorpe et al. [21] summarize the susceptibilities of what-you-know-based authentication such as text and graphical passwords. The threats include shoulder surfing which is made easier by high resolution phone cameras, dictionary attacks which are made easier by poor password choices, acoustic attacks on typing rhythm, and disclosure of password by the user through sharing or writing down to aid in later recall. ‘Who you are’ authentication traditionally relies on biometric keying such as the use of a fingerprint or iris scanning to authenticate to a system. The problem with this class of authentication methods as Thorpe et al. [21] point out is that they rely on a key whose lifetime is that of the owner. Various authors [4, 14] have discussed several attacks facing physical biometric systems on various levels in the authentication process. If biometric identity is compromised, then the vulnerability of the individual may be permanent due to the lack of a changeability property. As noted by Thorpe et al. [21], physical biometrics are not used for remote authentication.

'What you have' based authentication involves the use of a physical token often in the form of a smart card to authenticate oneself to a system. The problem in this authentication scheme is the fact that authenticating authorities have not found a way of consolidating their functions into a single universal token per single user which means the user must carry a separate token for every system that uses such an authentication scheme. As Thorpe et al. [21] note, this can be inconvenient for the user. The issuance and management of tokens is also an unrealistic cost for many systems, such as social media websites, with high user turnover and often free patronage.

Increasingly, combinations of these factors are used together in what is known as multi-factor authentication. Kiljan et al. [11] conducted a survey on 80 home banking sites, 60 mobile banking applications and 25 mobile banking sites in a study similar to a previous one they conducted in 2013 and compared the results. In their 2015 study they found that most banks in Europe, South America, and Oceania required the use of multiple factors, while most other regions seem to be more divided. However, they found that there was not much change in the overall use of knowledge and possession factors in both mobile applications and sites between 2013 and 2015 except for the introduction of possession-only authentication by a few banks. The authors found that passwords were popular in both multi-factor and single factor usage while PIN numbers were only applied when multi-factor authentication was used, a pattern which can be attributed to the lower complexity of PINs compared to passwords. The authors note that while biometrics based on physical characteristics can be used as an additional or alternative authentication factor for user authentication, the method is faced with disadvantages. These disadvantages include unwillingness of some people to use biometrics due to social stigma, and the limited number of non-replaceable characteristics which can also be absent if the user is disabled. Behavioral characteristics on the other hand are not applicable for initial authentication when based upon anomaly detection since the user has to do some activity first for anomaly to be detected. However, as the authors point out, analysis of usage characteristics such as usual time of login and known location can be used as part of initial authentication.

2.2 Password Authentication

Use of passwords is the most common form of authentication perhaps due to its low cost of implementation especially on unmonitored systems. In theory, passwords could offer a high entropy but user choices make it difficult to achieve. As an example, Thorpe et al. [21] discuss in their character based pass-thought system that assuming a textual password scheme where all 95 printable ASCII characters are displayed on a screen and the user must select a sequence of 8 characters, the size of the full pass-thought space is 958, approximately 52 bits could be achieved but the poor choice of passwords by users limits what can be expected.

In a study of web password habits conducted by Florencio and Herley [6] covering half a million accounts over the course of 3 months, users chose passwords with an average bit strength of 40.54 bits. Also, unless forced to do otherwise, the majority chose passwords that contained only lower case letters without any uppercase letters, digits, or special characters. Additionally, the average password was re-used in at least six different sites at times including phishing sites. It is notable similar user habits as related to passwords were found in a smaller study conducted almost two decades earlier [13]. In this experiment, user passwords were easy to crack as lengthy dictionaries could be scanned fast and words could be permuted in different ways. As an example, a dictionary of 250,000 words could be checked in under five minutes. He was also able to crack passwords from languages other than English and even less common words like "fylgjas." His observation was that users typically choose weak passwords, which was confirmed many years later by Florencio and Herley [6]. An explanation for this behavior relates to problems of password recall and recognition. As Forget et al. [7] discuss, more secure passwords are often difficult to remember. In attempting to solve this problem, they conceptualized the *Password Rehearsal Games (PRG)* based on their study of Brain Age games made by Nintendo. They discuss that Nintendo's Brain Age games which involve memory, language, and mathematical exercises, were inspired by neurophysiology and brain mapping research on cognitive functioning. In their work, Forget et al. [7] suggest that password rehearsal games could help users recall their real passwords better. While memory games are not themselves a new idea, their efficacy is not widely agreed upon. Melby-Lervåg and Hulme [17] conducted a meta-analysis of several studies on memory training and arrived at the conclusion that although memory training programs can yield reliable improvements on both verbal and nonverbal working memory tasks, these effects are likely to be short-term. They found that for verbal working memory, near-transfer effects are achieved but are not sustained when reassessed after a delay averaging roughly 9 months. Near-transfer effects are those reflecting in tasks closely related to the ones in the training program. For visuo-spatial memory, the pattern has not been as clear although a few studies suggest that modest training effects can occur and can last up to 5 months after cessation of training.

Another method that has been studied for improving brain function is the stimulation of the dorsolateral prefrontal cortex (DLPFC) using Transcranial Magnetic Stimulation (TMS). Bhattacharyya et al. [2] discuss in their review of neurotechnology that this kind of stimulation has been linked to improvements in basic cognitive functions, including working memory assessed through performance in the N-back task. The N-back task as described by the authors is a continuously performed task in which the subject is given a sequence of images and asked to identify a match within the sequence. For instance, 1-back is a comparison of the current stimulus with the previous one while 2-back is a comparison between the current stimulus and the one 2 steps back, that is the one before the previous one. As they point out, evidence of improvement varies widely across methods and studies. It appears that memory training games could require a lot of conscious effort and motivation while the effects are very moderate, do not last long and may even fail to occur and neurotechnology may be harder to access and require more specialized application with varied usability and results. This reduces the prospects of making password systems more secure through memory and cognition improvement techniques.

2.3 Authentication Using Physiological Measurements

In exploring possible alternatives to password authentication, physiological measures have shown the potential to expand the 'who you are' model of authentication which was previously confined to the physical properties of the entity being authenticated. This is due to uniqueness of physiological behavior to an individual, and the measurability of these physiological events. As Ikehara and Crosby [10] discuss, there are many physiological events that can be measured directly using sensors including eye movements, pupil size and skin conductivity. These measures can be used to identify various cognitive states including stress, fatigue, arousal, attention deficit and many others. In their experiments, they used a mobile eye tracking system and a desktop model to obtain gaze position and pupil size. They also used a custom designed electrically isolated physiological sensor system to obtain galvanic skin conductivity (GSR), peripheral temperature, relative blood flow and the pressures applied to a computer mouse. Identification of cognitive states of individuals could be used to authenticate them. The authors suggest that unexpected cognitive measures would lead to a prompt to the user to reauthenticate themselves. Further, the authors propose that if these measures can be obtained continuously, then a continuous authentication model can be created to prevent unauthorized users from slipping into a system and being able to use it. Recognition of various cognitive states has been studied in different contexts and efforts to automate the sensor data collection continue in various contexts.

Picard [19] developed a wristband for measurement of skin conductance, while they worked towards automating the recognition of stress and emotion. Their interest in electrodermal activity (EDA) measurements grew after they found in various tests that skin conductance correlated highly with stress levels. In their experiments focusing on children with autism, a group they selected because of its higher levels of response to stimuli, they saw among other observations that skin conductance measurements grew during tasks that increased cognitive or physical exertion. Conversely, skin conductance decreased during repetitive movements like swinging or rocking, suggesting relaxed feelings. In their work, they continually correlate the EDA data with brain data measurements for reference. As they note, brain studies have shown that a key part of the brain involved in emotion is the amygdala. Taking a closer look at literature in brain studies, many processes happening in the body can be correlated with a visible change in structure or otherwise measurable signal change in the brain. Gonzalez and Berman [8] discuss that brain mapping can be used to associate one physiological process with another or with occurrence of some event. Conversely, brain mapping can also be used to dissociate two or more processes by finding brain regions that respond differently to different experimental manipulations. Brain mapping also helps to draw connections between physiological function and respective anatomical structure in what is known as localization.

The authors suggest that brain imaging is important in research reliant on psychological factors because it enables optimization of techniques towards collection of good data. This is because brain imaging has enabled classification of cognitive actions and led to the understanding of the spatial temporal resolution dynamics. Each of the current brain mapping technologies has either a high temporal resolution or a high spatial resolution but not both. However, some researchers have combined brain mapping methods in order to obtain both optimizations. As Gonzalez and Berman [8] argue, the study of the relevant neuroscience is important when intending to collect and use brain data for various reasons; first it helps in understanding how to set up a good experiment environment that supports collection of good data, it also helps to know how to design questions in a way that can enable one to reach valid conclusions using data from brain mapping as well as how to design the experiment itself, putting in adequate constraints, and being cognizant of various confounding variables.

2.4 Neurofeedback of Recall and Recognition Functions

We now highlight recall and recognition which are the cognitive functions central to the 'what you know' authentication paradigm. Cabeza et al. [3], conducted an experiment to compare regions of the brain used for recognition and recall functions. They used positron emission tomography to take measurements while young healthy persons were recognizing or recalling previously studied word pairs. The researchers included some words not previously studied by the participant, to serve as a control to the experiment. Their experiment found that recall tasks caused a higher activation of blood flow in the anterior cingulate, globus pallidus, thalamus, and cerebellum, suggesting a role played by cerebellofrontal pathway in recall but not recognition.

Recognition on the other hand caused a higher activation in right inferior parietal cortex, suggesting a larger perceptual component in recognition than recall. They found that activations of frontal regions were indistinguishable between recognition and recall. As they discuss, this last observation corroborates the notion that frontal activations simply indicate attempts to retrieve some stored information but do not point to the specific mechanism of retrieval. Brain mapping can possibly expand not only the 'who you are' but also the 'what you know' paradigm of authentication because one will recognize or recall what they know.

2.5 Brainwave Based Authentication

Brainwave based authentication has been made possible by the progress made in brain computer interaction (BCI) research. BCI research started out with search for solutions for brain control of prosthetics for disabled patients. BCI interfaces link the brain's EEG signals with a computer [1]. The essence of brain computer interaction work is: observe a brain signal evoked by some stimuli, extract its features, translate or classify those features into recognizable command using signal processing and machine learning techniques Thorpe et al. [21]. As Bayliss and Auernheimer [1] found in a study comparing BCI under immersion in a virtual environment versus BCI while simply staring at a computer monitor, there were no significant differences between these two conditions.

A tool commonly used for signal acquisition is the electroencephalogram (EEG). The term electroencephalogram (EEG) is derived from combining ‘Electro’ meaning electrical activity, ‘encephalo’ meaning brain, and ‘graph’ for the picture [14]. As indicated by the name, the EEG measures the brain’s electrical activities. It does so using electrodes attached to the scalp. These electrodes are connected to a computer to display and store the measurements. The electrical signal is produced by the combined activity of large number of similarly oriented pyramidal neutrons. In other words the signal is the result of synchronous activity across a large group of cells (Personal Communication: Vibell Lecture Notes 2017). Each person’s brain patterns are unique and different from those of other people.

As [14] discuss, brainwave signals are usually decomposed in several frequency bands with each band signaling a particular brain activity. The authors summarize the broad categorizations of the EEG signal bands in their literature review: Gamma - active thought, attention, learning, visual perception, memory; Beta- Alert, Working; Alpha- Relaxed, Reflective; Theta-Drowsy, Meditative; Delta-Sleepy, Dreaming. The authors also summarize the different classes of brain signal: The Slow cortical potentials (SCP) which refers to slow brain signal typically from non-movement tasks from 300 s; The P300 evoked potential generated by auditory, visual & somatosensory stimuli in the parietal cortex region after 300 ms of stimuli exposure; The visual evoked potential (VEP) caused by sail changes in the brain resulting from visual stimulus such as flashing lights; The activity of neural cell which is a measure of firing rate of the neuron in the region of motor; The energy of the brain reflected by the energy of brainwaves at different frequencies; The acknowledge to mental task which is caused by a mental task such as solving an arithmetic expression or imagining a 3D object; The complex neuro-mechanism group is any combination of the other classes.

Feature classification is carried out using different mathematical techniques such as *fourier transformation* which enables signal representation in frequency bands such as delta, theta, alpha, beta, and gamma with each band being classified as a different feature [20], *auto-covariance* which involves finding features which distinguish one EEG signal from others, and other techniques.

The P300 brain signal has proved relevant and useful in cognitive biometrics because it reveals the change in mental state that occurs when a user recognizes some stimuli. Its discreteness property makes it useful for environmental control [1]. Meijer et al. [16] showed that mere recognition was sufficient to elicit a P300 response and that it was not essential that the recognized stimuli be important to the participant. In their experiment, they isolated mere recognition by having participants respond based on an irrelevant dimension of the stimuli such as faces of known public figures with comparison to people important to the participant and people not known by the participant. The authors note that stimuli referring to information relevant to the participant elicits a larger P300 than stimuli referring to incidentally acquired information.

2.6 Brainwave Based Authentication System Design and Security Proposition

The availability of low cost EEG sensors has motivated research work in brain computer interactions and brainwave based authentication. Chuang et al. [5] studied the efficacy of single-channel as opposed to multi-channel EEG signals, being that single channel devices are lower end versions of EEG devices. In their experiment, they used a consumer-grade headset that provided a single-channel EEG signal. They designed mental tasks for subjects to perform such as breathing, singing and listening and authenticated subjects based on performance in the specific tasks chosen for them. The authentication involved matching a sample to a pre-recorded identity. They designed a user matching algorithm adapted from the K-Nearest Neighbors (KNN) algorithm for coloring graphs, with their adaptation making the trial signatures the nodes, the subject identities the colors and the cosine similarity being the distance metric. They measured the false acceptance and the false rejection error rates. The findings revealed that single-channel EEG authentication can be just as accurate as multi-channel EEG authentication because single-channel signals do exhibit subject-specific patterns.

Thorpe et al. [21] focused on harnessing the P300 paradigm in their design proposal of a pass-thoughts system that authenticates by applying thoughts in the way that text passwords are traditionally applied to log into a device. Their idea was to use a thought based system as a natural 2-factor system where the changeable thought or measurable response to a stimuli is the first factor and physiological uniqueness of brain signal is the second factor. They proposed a system where the user would select a pass-thought, then to log in they would look at a character set on the screen where the characters would be highlighted one at a time and randomly. When the user sees part of their pass-thought highlighted their P300 would spike. The P300 spikes would be recorded and used to determine whether the user's P300 firing matched the expected template of that user's account's password i.e. after the user completes the pass-thought input, the hash of the pass-thought is compared to the stored pass-thought. They point out that although the size of the pass-thought space for this scheme is dependent on the number of characters on the screen and the number of screens that get presented to the user, in reality the message space is always curbed by user choices.

The security proposition in brainwave based authentication as in other physiological property based authentication is that brainwave patterns are less susceptible to forgery. This is due to various factors including that brain response events are unconsciously controlled, unique for each person and changeable e.g. by changing one's thoughts. As Thorpe et al. [21] argue, a login system such as pass-thoughts would be shoulder-surfing resistant, and also resistant to acoustic attacks and dictionary attacks. The authors are careful to note that although brainwave based authentication could offer better security guarantees than other methods like typing in text passwords, the method is also susceptible to some attacks such as social engineering as well as interception attacks in remote usage. In their coloring-graph-type user matching algorithm Chuang et al. [5] note that user identification proved harder than user authentication. That observation raises the question of whether an attacker could successfully forge identity once they know the custom tasks a system expects from a target. Brainwave based authentication is faced with other limitations as well.

2.7 Limitations on Brainwave Based Authentication

As noted earlier, low cost availability of EEG devices has made it easier to explore brainwave based authentication especially being that lower end EEG devices have been shown to reveal subject-specific brain patterns characteristics almost as well as the higher end tools. However, EEG based authentication has been reported to be a slow method of logging in to a system. Thorpe et al. [21] report that the P300 bit rate is 4.8 characters per minute which would make the login process noticeably slower. This could feel like a step in the backward direction for many and is one reason brainwave authentication may not have mass applicability for now. However, it is reasonable to view this as a short-term problem due to the rate of growth of bit processing power. Another problem is that EEG signal collection involves mounting the EEG headset on a user's head to make contact with the scalp. Although this is not considered invasive, it does limit mass applicability. Thorpe et al. [21] mention an interesting direction to explore, that is if the P300 signal could be collected using a touch pin pattern, a technique that could allow the scheme be integrated to a cellphone touchscreen. Another potential problem is that if the tasks are similar then user selection may converge on a similar pool of choices. However, when participants only had to answer a question by thinking of something, a rate of collision of user choices of thoughts was not identified.

2.8 Deception Detection in EEG Data

Meijer et al. [16] showed that mere recognition was sufficient to elicit a P300 response and that it was not essential that the recognized stimuli be important to the participant. However, they note that other studies exist which indicate that stimuli referring to information relevant to the subject elicit a larger P300 than stimuli referring to incidentally acquired information. These findings raise the question of whether it is possible to tell between those who honestly acquired or owned some piece of information such as a password and those who had acquired it disingenuously. Some progress has been made towards finding an answer to this question as wavelet analysis of EEG signals has been applied with some success in general deception detection. Merzagora et al. [18] investigated the capacity for EEG measurement to differentiate among the cognitive elements of truth and deception. Neither time-domain nor frequency-domain features revealed any significant difference between channels or responses. However, on analysis of wavelet domain features extracted from the EEG, they found that wavelet coefficients with a joint time-frequency distribution corresponding to the beta rhythm were able to discriminate true and false information in time windows from 300 to 1000 ms. They note however that their work is preliminary and would need larger samples sizes, more diverse protocols, and other considerations in future iterations of the experiment.

Khandelwal et al. [12] in their conceptual study also suggest that EEG could be used to detect basic lying. They reference other methods that already show results. For example, functional magnetic resonance imaging (fMRI) which records brain activity by identifying changes in brain blood flow and the metabolic rate has shown that the conflict between true and false information can be observed when imaging the brain. However, these studies do not reveal if disingenuously obtained information would be detectable. Although acquiring this type of information involves some dishonesty, such information is essentially not a lie.

2.9 Attacks on EEG Based Authentication

A study by Martinovic et al. [15] shows the feasibility of side channel attacks on EEG based authentication. In their study of the security implication of consumer grade BCI devices, they found that the signal captured by a consumer-grade EEG device can be used to extract potentially sensitive information from the users. In their experiment, the attack vector was third party developer applications in EEG-based gaming headsets which are low-cost and easily available in the consumer market. The threat model was the fact that the EEG devices developer API provided unrestricted access to the raw EEG signal and allowed applications complete control over the stimuli that could be presented to the users. The attacker in this case could be the ill-meaning third-party developer. The study investigated how third party EEG applications could infer private information about the users, by manipulating the visual stimuli presented on screen and by analyzing the corresponding responses in the EEG signal. They based the success of slipping in irrelevant stimuli to a user on the fact that P300 is elicited during stimuli that are personally meaningful to participants even though not defined by the task. This is consistent with what Meijer et al. [16] found in their literature survey that if the information had some meaning to the participant, P300 could be elicited without any instructions or tasks. In the experiment, the gaming device user who was the target of attack was probed to detect whether certain stimuli such as PIN number, bank name, and month of birth were familiar to or relevant for the user. They found that found that the entropy of the private information is decreased on the average by approximately 15%–40% compared to random guessing attacks. They suggest a remedy where the EEG application API is made more restrictive not giving third party developers access to raw data, a strategy that could limit developers both positively and negatively. Other suggestions include users consciously ignoring non-target stimuli, an expectation that may not be realistic.

2.10 Continuous Authentication Using EEG

As discussed, EEG measurement can reliably differentiate between different individuals. However, for the scheme to be applicable towards continuous authentication, there are still questions as to whether a user can be continuously re-identified correctly with changes in the environment over the short term and over an extended timeframe. If the EEG can continue to recognize a user across their changing cognitive states, then it can be applicable for continuous authentication.

Kumari and Vaish [14] in their review of methods in EEG based authentication note among the advantages of using the EEG signal that it can be collected continuously allowing for ascertaining that the subject is alive. They also note that if it is coerced out of subject the EEG signal will be distorted by stress. Additionally, since it is related to genetic information a stable unique pattern for each person can be attained over time. The stability factor is however still being studied. Gupta et al. [9], conducted a study investigating the stability of recognition features noting that the long-term invariance would be necessary for reliable implementation. In their work, they found among other results that the task design can influence stability and they suggested the use of Rapid Serial Visual Paradigm (RSVP) in task design for cognitive biometrics. On task usability, Kumari and Vaish [14] note in their work that this varies based on various factors including boredom level. Overall, the stability of recognition features in brainwave based biometrics has not been extensively studied.

With the eventual goal of developing a secure and memorable password authentication process, we are testing ways to effectively combine the uniqueness of physiological measures, such as brainwave patterns, with memorable augmented passwords. Our initial study was to use augmented passwords to elicit recognition and recall behavior.

3 Password Recognition and Recall Study

3.1 Setting

This initial study was conducted on a large-enrollment introductory computer science course at a research extensive university. Approximately 200–300 students enroll in this course each semester from over 30 majors. The course includes a lecture meeting and a laboratory component with a teaching assistant. One hundred fifty-seven students participated in the study.

3.2 Methods

To determine the recognition and recall accuracy of augmented passwords using font styles, we developed a system parallel to account password generation systems where users enter their passwords twice before using it for account authentication. We created a six-character string password with different font styles for students in the labs. The second character of the password string was modified for the different groups, no font style, bold, italicize, underline, and strikethrough. Students entered the password that was displayed on the projector twice on the first day to assess recognition and mirror password creation. On the second lab day, two days later, students entered their password from memory to assess recall and reflect account authentication. After entering the password on the second day, a survey was administered to determine the methods used to recall the password.

3.3 Results

Students had a recognition rate of 70% for no font style (plain text), 76% for bold text, 74% for italicize text, 75% for underline text, and 86% for strikethrough text (see Fig. 1). When asked to recall the password, students responded accurately 64% for no font style, 93% for bold text, 91% for italicize text, 94% for underline text, and 76% for strikethrough text. Performance improved between recognition and recall for bold, italicize, and underline text by 17–19%. Conversely, performance decreased for no font style (−6%) and strikethrough (−9%).

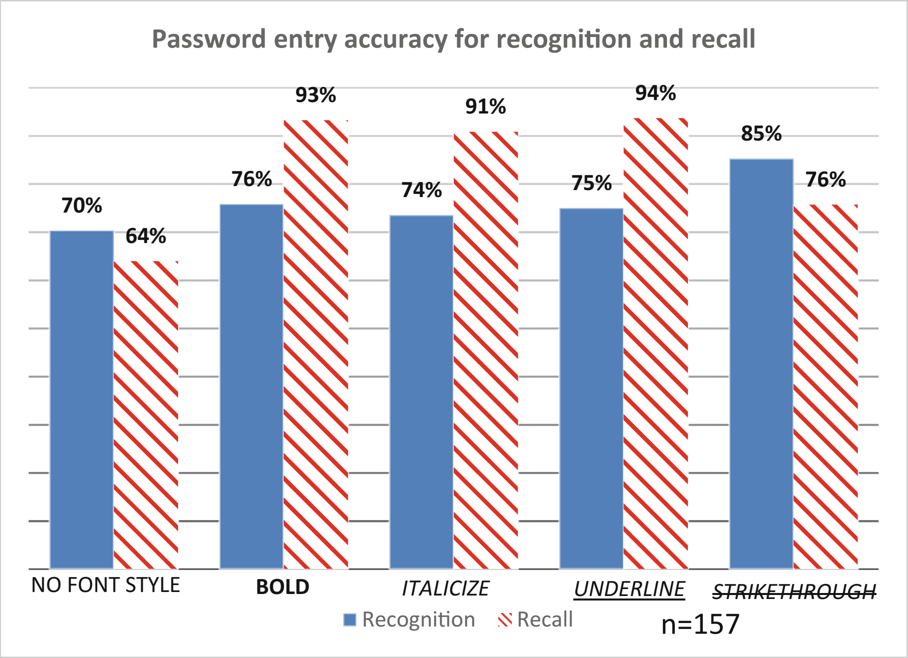

Fig. 1. Password accuracy for recognition and recall

Augmented password recall accuracy was higher than the non-augmented passwords with bold, italicize, and underline augmentation having over 90% recall rates and strikethrough having a 76% recall rate. The researchers believe that the augmented characters were distinctive, which made the password string more memorable for participants. The strikethrough augmentation had the lowest recall rate of the augmented passwords which could be attributed to its less use compared to bold, italicize, and underline text. Based on the greater recall rate, the authors believe that augmented passwords could be used in practice. By adding augmented characters to passwords, the total number of possible characters will increase from 95 ASCII characters [21] to 475 characters which enhances password strength.

Recognition accuracy for augmented passwords were also higher than the recognition rate for traditional passwords. Similar to recall, the authors believe that the higher recognition rate is based on one of the characters including augmentation, which helped the participant to focus on the string and accurately replicate it. The increased accuracy for augmented password strings may support its usage in multifactor authentication environments, particularly with a secondary authentication method such as one-time passwords [11].

When asked about recall strategies, 62% of the students took a picture of the password with their phone to review (see Fig. 2). Sixty-one percent mentally repeated the password to visualize the it and improve recall on the second day. Forty-eight percent of the students verbally repeated the password to themselves to practice recalling the string and font style. Twenty-four percent hand wrote the password in their notes for future review. Twenty-two percent used mnemonics to improve recall. Under 10% repeatedly practiced writing the password on paper or typing it on a computing device. Overall, the most popular strategies to practice recalling the password were mentally repeating the string (62%) and verbally repeating the string (48%). A majority of the students (61%) used their cell phone to initially capture the password as a reference tool, but did not directly use it for practice.

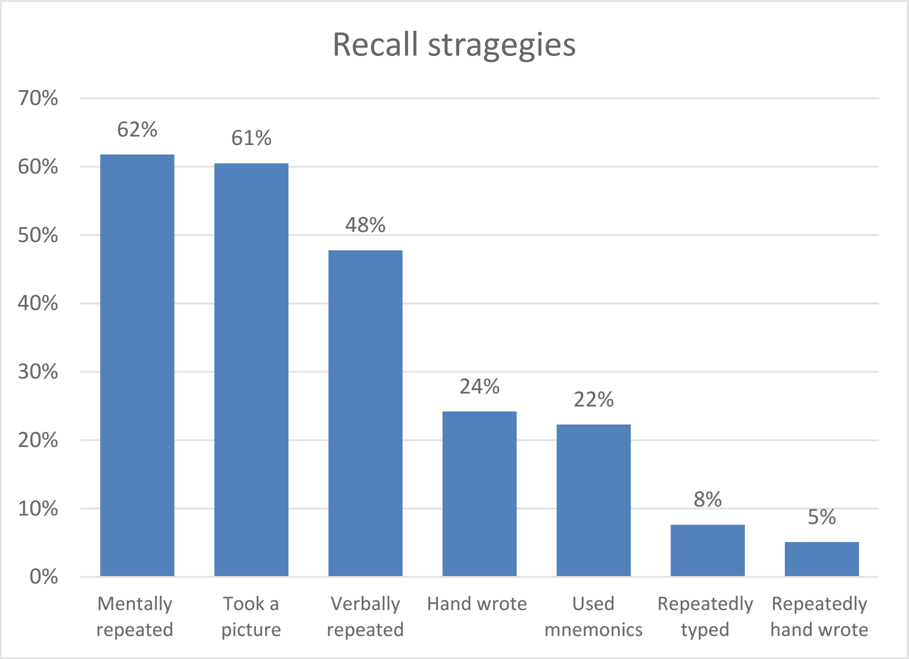

Fig. 2. Recall strategies

Given the recall strategies the participants employed, the authors suggest matching rehearsal strategies to the users' practices rather than providing users with practice tools such as rehearsal games [7]. Even though a wide range of rehearsal techniques can improve password recall [17], embedding rehearsal techniques in the users' everyday practices would likely lead greater amounts of practice rather than having to rehearse using a technique that is not a typical practice.

4 Password Recall and Recognition Study Using Physiological Measurements

In our proposed next study, whose results are not presented here, we repeat the above study, taking measurement of physiological data elicited by the recall and recognition processes during usage of the system. We can draw physiological patterns but are they accurate enough to be used to authenticate users? The task used in controlling the measurements is their usage of the augmented password system. In essence, the augmented password system provides the first factor while the physiological measures provides the second factor in this study.

4.1 Methodology

We are collecting data from 30–50 participants. Three standard-size disposable sensors will be applied to the forearms to measure heart rate. Two standard-sized disposable sensors will be attached to the palm of the subject's non-dominant hand to measure skin conductance. Two sensors will be attached to skin over the orbicularis oculi muscle just below the eye. Two small sensors will also be applied just above the participant's left eyebrow to measure frown muscle activity. Brainwave activity will be recorded over the course of the experimental procedure using an Emotiv EEG data collection headset (http://www.emotiv.com/researchers/). The protocol begins once the physiological data collection, sensors are applied.

The task is to ask individuals to either create and transform a password or to recognize a password transformation previously created by themselves, or to recognize a password, pattern, arithmetic expression previously disclosed to them and modify it in a predefined and pre-discussed way. A session constitutes a combination from the 4 tasks: create, modify, recognize or recall some distinct object such as a character, shape or image. At the end of the tasks, the participant is given a feedback questionnaire. Once the results are analyzed, we will study the stability of these measurements over the short and longer terms and how they could be used in a continuous authentication model.

References

1. Bayliss, J.D., Auernheimer, B.: Using a brain-computer interface in virtual and real world. Proc. Ninth Int. Conf. Hum.-Comput. Interact. **1**, 312–316 (2001)
2. Bhattacharyya, R., Coffman, B.A., Choe, J., Phillips, M.E.: Does neurotechnology produce a better brain? Computer **50**(2), 48–58 (2017). doi:10.1109/mc.2017.49
3. Cabeza, R., Kapur, S., Craik, F.I.M., McIntosh, A.R., Houle, S., Tulving, E.: Functional neuroanatomy of recall and recognition: a pet study of episodic memory. J. Cogn. Neurosci. **9**(2), 254–265 (1997). doi:10.1162/jocn.1997.9.2.254
4. Chen, L., Pearson, S., Vamvakas, A.: A trusted biometric system - PDF. http://docplayer.net, http://docplayer.net/33351165-A-trusted-biometric-system.html. Accessed 18 Feb 2017

5. Chuang, J., Nguyen, H., Wang, C., Johnson, B.: I think, therefore i am: usability and security of authentication using brainwaves. In: Proceedings of the Workshop on Usable Security, USEC 2013 (2013)
6. Florencio, D., Herley, C.: A large-scale study of web password habits. ACM, New York (2007). doi:10.1145/1242572.1242661. ©2008
7. Forget, A., Chiasson, S., Biddle, R.: Lessons from brain age on password memorability. ACM, New York (2008). doi:10.1145/1496984.1497044. ©2008
8. Gonzalez, R., Berman, M.G.: The value of brain imaging in psychological research. Acta Psychol. Sin. **42**(1), 111–119 (2010). doi:10.3724/SP.J.1041.2010.00111
9. Gupta, C.N., Palaniappan, R., Paramesran, R.: Exploiting the P300 paradigm for cognitive biometrics. Int. J. Cogn. Biometrics **1**(1), 26–28 (2012). doi:10.1504/IJCB.2012.046513
10. Ikehara, C.S., Crosby, M.E.: Physiological measures used for identification of cognitive states and continuous authentication. In: CHI 2010 (2010)
11. Kiljan, S., Simoens, K., Cock, D.D., Eekelen, M.V., Vranken, H.: A survey of authentication and communications security in online banking. ACM Comput. Surv. **49**(4), 1–35 (2016). doi:10.1145/3002170
12. Khandelwal, R.J., Mahajan, J.D., Bombatkar, U.P., Badhe, S.G.: Analysis of EEG signals for deception detection. Int. J. Adv. Res. Elect. Electron. Inst. Eng. **5**(2) (2016). doi:10.15662/IJAREEIE.2016.0502038
13. Klein, D.V.: Foiling the cracker: a survey of, and improvements to, password security. In: Proceedings of the 2nd USENIX Security Workshop (1990)
14. Kumari, P., Vaish, A.: Brainwave based authentication system: research issues and challenges. Int. J. Comput. Eng. Appl. **IV**, I & II (2014). ISSN: 2321 - 3469
15. Martinovic, I., Davies, D., Frank, M., Perito, D., Ros, T., Song, D.: On the feasibility of side-channel attacks with brain-computer interfaces. In: The Proceedings of the 21st USENIX Conference on Security Symposium (2012)
16. Meijer, E.H., Smulders, F.T.Y., Wolf, A.: The contribution of mere recognition to the P300 effect in a concealed information test. Appl. Psychophysiol. Biofeedback (2009). doi:10.1007/s10484-009-9099-9
17. Melby-Lervåg, M., Hulme, C.: Is working memory training effective? A meta-analytic review. Dev. Psychol. **49**(2), 270–291 (2013). doi:10.1037/a0028228
18. Merzagora, A.C., Bunce, S., Izzetoglu, M., Onaral, B.: Wavelet analysis for EEG feature extraction in deception detection. In: 2006 International Conference of the IEEE Engineering in Medicine and Biology Society (2006). doi:10.1109/iembs.2006.260247
19. Picard, R.W.: Automating the recognition of stress and emotion: from lab to real-world impact. IEEE Multimedia **23**(3), 3–7 (2016). doi:10.1109/MMUL.2016.38
20. Safont, G., Salazar, A., Soriano, A., Vergara, L.: Combination of multiple detectors for EEG based biometric identification/authentication. In: 2012 IEEE International Carnahan Conference on Security Technology (ICCST) (2012). doi:10.1109/ccst.2012.6393564
21. Thorpe, J., van Oorschot, P.C., Somayaji, A.: Pass-thoughts: authenticating with our minds. ACM, New York (2005). doi:10.1145/1146269.1146282. ©2005