Reflexive Memory Authenticator: A Proposal for Effortless Renewable Biometrics

Nikola K Blanchard, Siargey Kachanovich, Ted Selker, Florentin Waligorski

Reflexive Memory Authenticator: a proposal for effortless renewable biometrics

Nikola K. Blanchard[1], Siargey Kachanovich[2], Ted Selker[3], and Florentin Waligorski

[1] Digitrust, Loria, Université de Lorraine Nikola.K.Blanchard@gmail.com
www.koliaza.com
[2] Université Côte d'Azur, INRIA Sophia-Antipolis, France
[3] University of Maryland, Baltimore County

Abstract. Today's biometric authentication systems are still struggling with replay attacks and irrevocable stolen credentials. This paper introduces a biometric protocol that addresses such vulnerabilities. The approach prevents identity theft by being based on memory creation biometrics. It takes inspiration from two different authentication methods, eye biometrics and challenge systems, as well as a novel biometric feature: the pupil memory effect. The approach can be adjusted for arbitrary levels of security, and credentials can be revoked at any point with no loss to the user. The paper includes an analysis of its security and performance, and shows how it could be deployed and improved.

Keywords: Eye biometrics · Authentication · Adaptive systems

1 Introduction

Until recently, biometric authenticators seemed to be the holy grail for access security. Improved sensor technology made available new alternatives such as iris and eye muscle signature, with the most accurate approaches reaching error rates below 0.01%. Unfortunately, even these top biometric solutions suffer from two important problems. The first is that an adversary can record and replicate the iris or even simulates eye muscle motions to a present as a user. The second problem is that even if this does not happen, each person today needs independent security for a large array of services. Aggregating the authentication would require some independent trusted reliable intermediary service. Such a service that is always available for all devices and services a person needs to access easily exposes a user to access failure, as well as other single point of failure problems. An ideal approach would allow a person to create new authentication mechanisms if old ones get compromised or to independently access services without compromising other services' access methods, which eliminates most biometrics. This paper works to demonstrate a new kind of biometric approach that could allow ongoing creation and cancellation under attacks, by using an unconscious learning and memory biometric feature.

Contributions. We propose a mutable reflexive biometric authentication system that does not suffer from credential theft and re-use, with arbitrary security due to a time-security trade-off. We analyse its security against multiple standard attacks, and the principal obstacles to its implementation in practice. This proposal is presented to motivate development, and although the system could be used today, empirical tests will be needed to validate and optimise its performance.

This paper is structured as follows: Sections 2 and 3 go over the related work for the two main authentication methods on which the protocol is based. Section 4 introduces the specific biometric mechanism used, and Section 5 goes over the details of the protocol. Section 6 analyses the resistance of the protocol to multiple kinds of attacks. Finally, extensions of this protocol to different use-cases, vulnerabilities, and potential improvements are discussed in Section 7.

2 Challenge-based authentication

2.1 Text challenges

Typical challenge-based authentication uses text questions: requesting answers to a series of questions or the completion of a list of tasks. Such approaches can achieve a relatively high level of security, with a higher promised level of usability than common passwords. This idea has been around since at least the early 1990s, initially as a list of personal questions [49].

This kind of system suffers from multiple issues, however:

- It is vulnerable to targeted attacks when the information is available [21].
- Free-form answers can lead to high error rates and frustration as people might misremember the exact spelling they used [43].
- To achieve high entropy, a potentially long sequence of challenges is needed. This requires more time and effort from the user and increases the system complexity [21].
- A large set of potential challenges is needed to avoid repetition of challenges between different services. User-provided challenges are also riddled with usability and security issues [22].

As such, text challenges have been superseded by different systems, based on intrinsic human visual pattern recognition abilities.

2.2 Graphical challenges

The main alternative to text challenges is visual — or graphic — passwords, where the user is confronted with a sequence of images and has to react, for example, by identifying known pictures [20], especially pictures of faces [6]. An alternative is to click on certain zones in a sequence of pictures, which can either come from an image corpus or be automatically generated [7, 48]. Some research has also looked at mixing different methods and mnemonics, such as storytelling plus visuals [37] or sound-augmented visual passwords [46].

This does not solve all the problems mentioned, however:

- It still requires either more complex challenges or a long sequence of challenges.
- Any system used by multiple service providers encounters the same risk of challenge re-use.
- Depending on the structure of the interaction, the systems are generally quite vulnerable to another person or camera recording what the visual challenge is by "shoulder-surfing" [28].
- Attempts at limiting shoulder-surfing impose strong constraints on the image set sizes [1], and come with an entropy cost.

Techniques inspired by these challenges are still present in the forms of CAPTCHAs, often in conjunction with passwords systems to frustrate automated attacks through rate-limiting [18, 24]. While they are present in multiple popular commercial solutions, such systems have not solved the central issue of authentication. We now turn to biometric authentication, which has been considered as a lower-effort security approach and plausibly an ultimate alternative to passwords.

3 Biometric authentication methods

For the purpose of authentication, a wide array of biometrics features has been used, going from hand shape to finger-print, voice print, or typing patterns. These methods have been used for decades, initially with limited uses in specific high-security sectors, such as banking or the military in the 1970s [30]. Their prevalence has increased dramatically in recent years, with more than 40% of users unlocking their phones through fingerprints or face recognition in 2018 [17]. A central issue to biometric authentication is the possibility to steal biometric information and use it later in what is called a *replay attack*. A large amount of work has been done to solve this, going from storing data in a way that is not directly re-usable [8, 33, 29] to using parallel systems to make sure that the sensor is not being fooled by a previously captured video [40, 27].

3.1 Error rates

Comparing biometric features and authentication systems requires a common metric. The most frequently used metric depends on two error rates: false rejection rate (FRR) and false acceptance rate (FAR). The false rejections, although not being a critical security issue, are a source of frustration of the users. The false acceptances, on the other hand, are a security failure. The two error rates are related: the stricter the system is, the lower the FRR and the higher the FAR become. Hence, we generally use the equal error rate (EER), the tolerance level for which FAR and FRR are equal. These rates are generally within 1% and 6-7% for any kind of authentication except for the iris-based ones, which have 0.01% EER but — like most classical biometrics — are not renewable and are vulnerable to theft. Even multimodal biometrics — where one uses multiple sources

and biometric features for liveness detection and improved error rates [41] — rarely improve below 0.2% EER [8, 16, 42]. Making the strong assumption that the user data are quite well-distributed — which is far from guaranteed — this corresponds to a min-entropy below 7 bits, on par with typical password systems. Moreover, most of the EER mentioned in papers on biometrics are against non-optimised adversaries: for a given set of user patterns, they check which proportion would be accepted as sufficiently similar to another user. An adversary that can compute an optimal distribution of fake patterns to cover the space of user data points more efficiently might get a success rate high enough to impersonate more than 10% of users despite a three-strike policy[4].

3.2 Eye and reflexive biometrics

After problems were discovered in fingerprint-based authentication, focus shifted to eye biometrics, with more than a hundred papers published on the subject in the last decade. Most of the research has been on iris recognition [4], where the unique patterns present in the iris allows for a much lower EER. More recently, eye movements have received a lot of interest, as muscular performance is quite distinctive [3, 25, 16]. Despite the much improved EER, the unchangeability of the underlying biometric pattern stays an intrinsic problem for nearly all biometric authentication systems.

As such, some of the proposed systems have been inspired by challenge systems. Notably, multiple systems were developed based on gaze analysis, which concentrates on how the eye moves when faced with specific images [15, 12]. In 2016, Sluganovic *et al.* proposed a challenge-based eye movement system [47], in which the server creates challenges in the form of a single dot quickly moving on a screen. As the point's location is random, it prevents replay attacks. The speed and patterns in the eye's movement are characteristic of the user's muscle function and allow them to authenticate them. This uses the user's unconscious reflexes, which means that it is quite low-effort to the user. However, the system still depends on a hidden model of the user's muscles. As such, it is vulnerable to an adversary that can compute a sufficiently accurate model of the user. Once this model is computed, it is impossible to reset the stimulus pattern. This means that the user cannot safely use that biometric on this service, or any other service, potentially compromising dozens of accounts.

To this date, there seems to be only one type of biometric authentication systems that are based on partially unconscious actions while being resettable. That is, where the stimulus and the reaction pattern can instantly be changed if they become compromised, just as one resets their password. These systems are all based on electro-encephalography (EEG), and tend to give an arbitrary task to the user before recording their electrical brain patterns — which are not consciously controllable — while they do so [2, 32, 10]. Alas, they suffer from common EEG drawbacks [11]:

– they tend to have high EER;

[4] Meaning that the person trying to authenticate is blocked after three failed attempts.

- they are costly and require specialised equipment that can be hard to set up;
- they require an extended time to capture and process the signals;
- they are not entirely stable over extended time periods.

Our idea is to create reflexive challenge biometrics that rely on a different biometric feature that has not been used previously for this purpose. Results on this feature from the psychological literature are presented in the next section.

4 The pupil memory reflex

The interactions between memory and eye behaviour have been studied for more than half a century [34, 36, 39] and are still a subject of ongoing research [23, 9, 13]. In 1967, Roger N. Shepard showed that recognition memory for pictures vastly exceeded recognition memory for words. A week after having been shown a set of 600 pictures, users who were shown two pictures and were asked to select the ones they had seen previously were correct 87.0% of the time. Even after four months without being shown pictures, they still managed to be right 57.7% of the time [34]. 5 years later, Geoffrey R. Loftus showed that pupil patterns could predict how well remembered an image would be [31]. Part of this memorisation is conscious, but some unconscious processing is also involved [19].

The feature central to the Reflexive Memory Authenticator protocol is quite simple: when presented with a stimulus, the pupil contraction reflex indicates how *new* the stimulus is to the user. More precisely, the pupil starts contracting between 200ms and 300ms after the stimulus starts. After this contraction and depending on whether the stimulus is still present, the pupil dilates back to its baseline over the course of a few seconds.

The contraction effect tends to be faster with novel stimuli, in which case it also takes more time to get back to the baseline. This is directly influenced by how familiar the image is. This effect has been shown through both declarative experiments — where the user states whether the image is familiar — and free viewing — where the already-seen images are recorded. In experiments performed by Naber, Frässle, Rutishauser, and Einhäuser [35], 48 participants were shown a list of pictures to memorise, and were later shown some of those pictures or new pictures randomly, while their pupil behaviour was recorded. Figure 1 shows the evolution of pupil size during retrieval on the right. Two main curves show this effect — depending on whether the user judged the picture familiar or not — and confidence intervals, which start diverging while the image is still shown (before the 1s mark). Figure 2 on top shows a similar curve with curve slopes.

A second effect also shown in the same study was that, during memorisation, pupil size can also serve as an indicator of whether the image would later be remembered. This is shown on Figures 1 on the left and 2 on the bottom.

An interesting effect, shown in [5], is that this effect is strongly modulated by the emotional content. Violent and erotic images elicit stronger and slightly

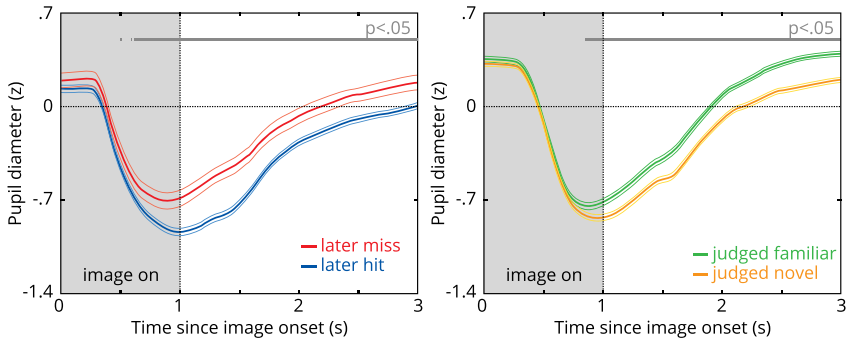

Fig. 1. Figures redrawn from [35, Figure 3A (left) and 4A (right), Experiment 1], showing the evolution of the pupil size during the memorisation phase (left) and retrieval phase (right). The red curve corresponds to an image that the user later forgets, and the blue one to a picture that is remembered. The green curve corresponds to a picture that the user remembers, and the yellow one to a picture that is perceived as novel. The grey area corresponds to when the images are on screen.

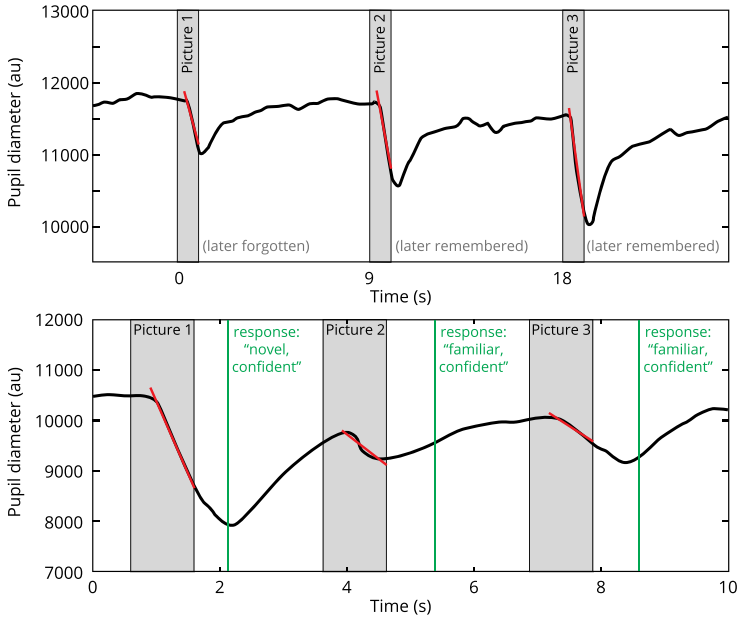

Fig. 2. Figure redrawn from [35, Figure 1B (top) and 1C (bottom)], showing the evolution of the pupil size during the memorisation and retrieval phase. The slopes vary depending on whether the image will later be judged as novel (top) or is being judged as novel (bottom) — and how confident the user is in that judgement (not shown here). The grey areas correspond to when the images are on screen.

different responses. Image content as well as uniqueness will affect the protocol, and care has to be taken on the choice of image database.

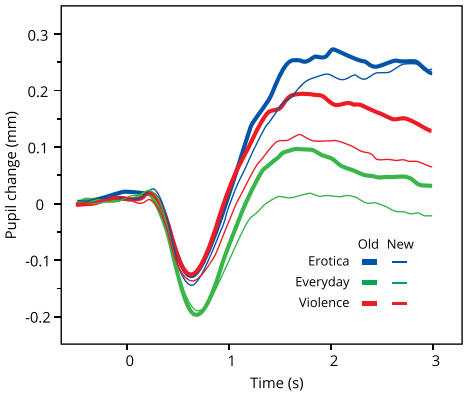

Fig. 3. Figure redrawn from [5, Figure 1], showing the evolution of pupil size as a function of time, novelty of stimulus, and emotional content. The image is shown for 3 seconds starting from 0 (the baseline is shown for 1s before the stimulus).

Without user effort beyond observing a sequence of images, this method can reliably decide whether the user is familiar with an image that might have previously been shown. The main question is how quickly this decision can be made, with most experiments Many experiments leave multiple seconds of rest for the pupil to return to baseline dilation, showing only one new image every three seconds, which allows them to know quite accurately whether the image was novel. This delay depends on cognitive and perceptual phenomena which are affected by factors including sleep, mood and intoxication. More experimentation may reveal further constraints on image recognition.

With all the building blocks in place, it's now time to introduce the Reflexive Memory Authenticator protocol.

5 Using reflexive pupil dilation for authentication

The protocol has two different modes of functioning: when the user registers for the first time, and when they try to authenticate afterwards.

5.1 Basic protocol

Registration. At the registration phase, the user provides their username, and the system selects a set of images (say, 30) and records that they correspond to

the user. The server tells the user to look attentively at the following pictures and shows them one by one for 1.5 seconds each[5].

Authentication. Each time the user tries to authenticate, the protocol works as follows:

- The system computes two lists of images. The first comes from the set of known images (based on the ones recorded in the registration phase), and the other comes from a database of never-seen-before images.
- In a series of rounds, an image is selected from one of the two lists, with probability 1/2 for each.
- The image is shown to the user for a recognition period of 1s. The screen then becomes blank for 1s to allow the user to return to their baseline.
- The system evaluates if dilation of the user's pupil corresponds to whether the shown image is known or unknown to the user.
- The system estimates the probability that the person who is trying to authenticate is indeed the user.
- If the probability exceeds a certain threshold, the system logs the user in.
- If more than a reasonable number of images (e.g. 50) have been shown or the probability is below a second threshold (indicating a very high probability of spoofing attempt), the system requires a CAPTCHA and warns the user of the attempt.
- Otherwise, the system chooses another image to show to the user from one of the two lists at random.
- If the user manages to get authenticated but had the wrong reaction to at least one unknown image, the one with the strongest reaction is added to the list of known images.

In practice, many explicit and implicit parameters that impact the performance of the Reflexive Memory Authenticator, which are covered below.

5.2 Implementation constraints and parameters

Before implementing this protocol in practice, here are the questions we must ask:

- Which images should be considered?
- How long should each image be shown, and how long should the resting period between images be?
- How do we ensure that the protocol eliminates noise coming from pupil size variability due to environmental conditions (such as glasses, camera characteristics, lighting variations)?
- Should known and unknown images be shown with the same probability?
- Which thresholds should govern acceptance, rejection, and continued testing?

[5] This is enough for the users to have high memory performance as in [35], while still being faster than nearly all password composition policies [44]

- How can targeted attacks be prevented?
- What should be the protocol for retiring images from the known set?
- How should the system keep track of which images are treated as known?

We will go over the first three questions here, before addressing the last four in Section 6.

Image types and sources. Natural scenes — for example, pictures of mountains, flowers or clouds — have been used in multiple studies [35, 23, 5] and form a common baseline. However, emotionally loaded images can elicit different reactions [5], and this could affect the system, both negatively or positively.

The system requires many unseen images for each login attempt. It then needs appropriately large databases to avoid the user seeing an image twice and being too familiar with it. For example, consider 20 authentication attempts per day, each with 20 novel images. Assuming that an image can be reused after six months, this would require 72000 images to be drawn without repetition. It could easily be done with the multiple online databases numbering in the millions of public domain images — such as Wikimedia Commons (https://commons.wikimedia.org), Snappygoat (https://snappygoat.com) or Free-images (https://free-images.com).

For the images to be drawn at random with little to no repetition, we would have to avoid the collision [26]. This would require close to 4 billion images, so the server needs to store at least partial information on the images seen. Subsection 6.6 expands on how to do this.

Time parameters. A parameter with a direct linear impact on usability is the delay per image. For example, each image can be shown for 1s, with a rest period of 2s, as has been done in previous psychological studies [35]. This means that to show 20 images — a lower bound to get the equivalent of 20 bits of security — a whole minute of authentication would be required. To keep a high level of usability, making the authentication process no-effort is not enough — it should also be quite fast, to avoid disturbing the user's workflow. The problem is that the shorter the time allowed for both presentation and rest, the harder it becomes to discriminate between the two contraction modes corresponding to a known or unknown image.

A lowered accuracy could still improve security by showing images at an increased rate. Based on previous work, an upper bound on the frequency, assuming no resting period, would be around 3 images per second [35]. For example, instead of a 95% classification accuracy in 3s, a system with 75% accuracy in 0.5s could take much less time to authenticate a user, depending on the actual number of errors. This kind of frequency brings two problems, however. First, it provides less data on an earlier time frame, which shows a less marked pupil memory effect. Second, it means that there is an interference because of the lack of resting period. This requires much more advanced statistical models to handle. One image per 3s is doable today but finding optimal parameters would require additional empirical studies.

Handling environmental variability. One common issue with eye biometrics is that capturing software has to accommodate for a large variability in real data. For example, pupil sizes react to cognitive load [13], but also to ambient light, alcohol and drug use, and mood. Because of this, most experiments control the luminance levels and try to keep them constant across all stimuli [19, 38]. One way to handle this in our context is to show a grey screen for a few seconds before authentication (or measure pupil sizes while the user types their login). Alternatively, we could show two or four initial images — half of them known, the others unknown — and use the reactions as a baseline for the rest of the authentication process.

6 Error tolerance and security considerations

6.1 Kinds of errors

The protocol that we described in Section 5 is prone to various errors, which can be classified into four types:

- *User false negatives*, where the user is not recognising an image that had previously been shown.
- *User false positive*, where the user recognises an image that is supposed to be unknown, as they've seen it before by coincidence (for example, by seeing it on someone else's screen).
- *System misclassification*, in which the pupil dilation is badly interpreted.
- *Sensor or environmental error*, where the hardware has a bug or something prevents the capture (because the user suddenly turns their head for example).

Probabilistic formalism. To be formal, we can integrate the previous errors into probabilities that the user is correct or not, depending on what is shown to them.

The probabilities that we take into account are the following:

- The base probability p_u of being the user. We use the value $p_u = 0.5$ in the calculations in the following.
- The probability p_s of the user to successfully classify an image. Unless stated otherwise, we assume that this probability is 0.95. The analogous probability for the adversary is fixed to be 0.5 throughout the paper.
- The probabilities p_x and $p_y = 1 - p_x$ of being shown an unknown (respectively known) image.
- The probabilities p_{x_0} and $p_{x_1} = 1 - p_{x_0}$ that the user does not recognise (respectively recognises) an unknown image.
- The probabilities p_{y_0} and $p_{y_1} = 1 - p_{y_0}$ that the user does not recognise (respectively recognises) an already known image.

The next question is whether p_x should be equal to p_y.

6.2 Showing more unknown or known images

Let us now consider a model in which the two probabilities p_x and p_y are not necessarily equal, and the adversary classifies any image as "unknown" with a probability x and as "known" with probability $1 - x$. We then get the following result:

Lemma 1. *The optimal strategy for the adversary is to classify every image as "unknown" if $p_x > p_y$, and as "known" if $p_y > p_x$.*

Proof. Without loss of generality, let us assume that $p_x > p_y$. This implies in particular that $p_x > 0.5$. In this case, the probability for the adversary to successfully authenticate after being shown n images is:

$$p'_s(x) = p_x x + (1 - p_x)(1 - x) = (1 - p_x) + (2p_x - 1)x.$$

Because $p_x > 0.5$, the function p'_s increases when x increases. Therefore, the optimal strategy for the adversary is to set $x = 1$.

With the optimal strategy, the probability for the adversary to succeed the authentication after being shown n images is $\max(p_x, p_y)^n$. As such, we have an interest in setting $p_y = p_x = 0.5$, which minimises this probability.

6.3 Handling the probability of an error

In our first model, we assume that $p_x = p_y = 0.5$. In addition, the adversary in this model randomly guesses whether an image is known or unknown to the user with probability 0.5.

We are interested in comparing the probabilities of successful authentication for the user and the adversary. These probabilities depend on two parameters: the number n of shown images and the number e of errors tolerated by the system. The general formulae for the probability of the successful authentication for the user and the adversary are:

$$\sum_{i=0}^{e} \binom{n}{i} (1 - p_s)^i p_s^{n-i} \text{ and } \sum_{i=0}^{e} \binom{n}{i} (0.5)^n \text{ respectively.}$$

Figure 4 shows the plots for success probabilities with $e = 0, 1, 2$ and $p_{x_0} = p_{y_1} = 0.95$.

6.4 Adaptive error probability

As seen on Figure 4, even by tolerating two errors, we eventually deny access to some users. As such, it is better to use an adaptive system where the probability of being the adversary is computed after each round.

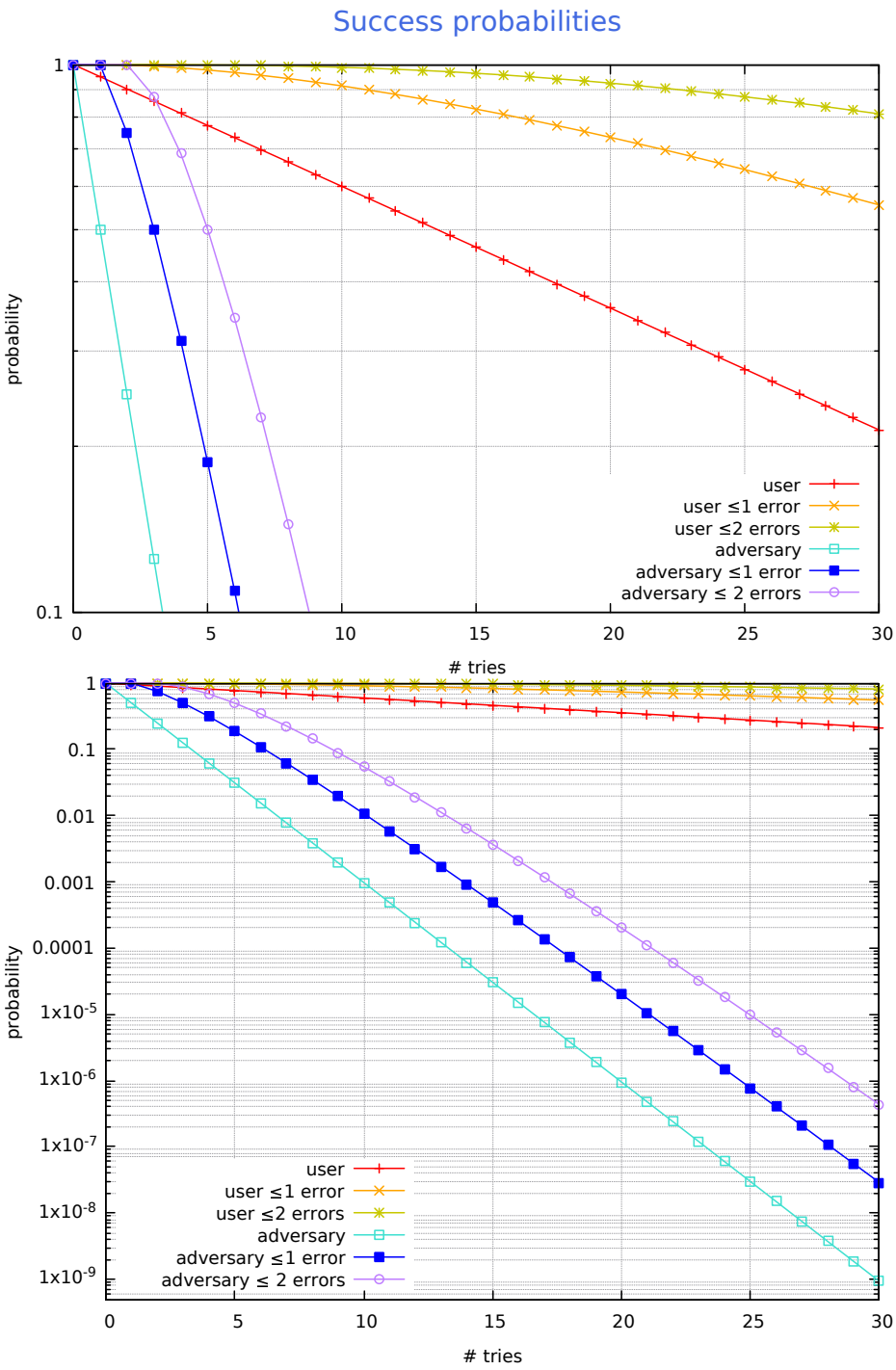

Fig. 4. Success probabilities of the user and an adversary to authenticate in the system, where different curves correspond to the number of errors tolerated by the system. Note that the probability axis is log-scaled. The same curve are shown again on the bottom with a larger logarithmic scale.

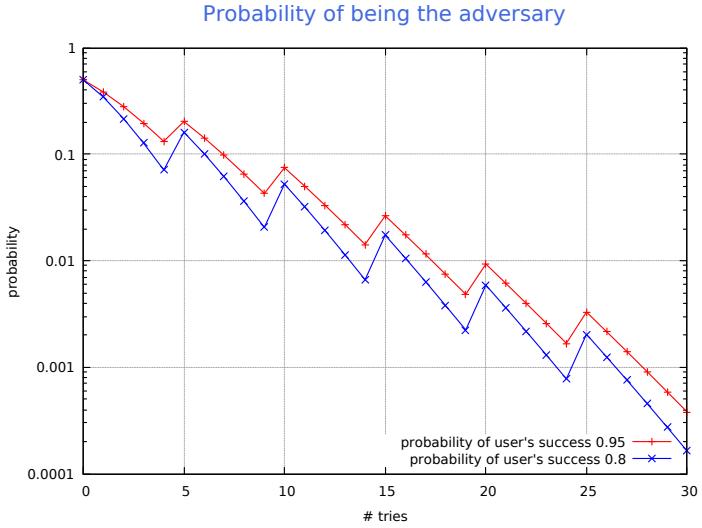

Fig. 5. The probability of the person who tries to authenticate being an adversary after an error occurred after each 5 images. The curve above and below take as base probability p_s of the user to be correct to be equal to 0.95 and 0.8 respectively.

The probability of being the adversary after n shown images with at most e errors can be found using Bayes' theorem:

$$\frac{\sum_{i=0}^{e}\binom{n}{i}(0.5)^n(1-p_u)}{\sum_{i=0}^{e}\binom{n}{i}(1-p_s)^i p_s^{n-i}p_u+\sum_{i=0}^{e}\binom{n}{i}(0.5)^n(1-p_u)}.$$

We ran exact numbers for a user that tries to authenticate but is misclassified every fifth image. Figure 5 shows how the probability of being a real user evolves in this context, and that it depends weakly on the server's stored probability that a user is misclassified. Even in a scenario where the user makes a mistake every five pictures — much higher than real data would indicate — the system has a lower error rate than all current biometric authentication systems in at most 27 challenges.

6.5 Preventing targeted attacks

A brute-forcing adversary has an exponentially small probability of success, as long as they don't remember which images have been shown. However, an adversary could memorise previously shown images. Let us denote by N the total size of the pool of known images, which could be estimated by the adversary, and by N' the number of images seen by the adversary. Once an adversary sees an image, necessarily this image is known to the user. Therefore, the adversary always classifies such an image as "known" if it appears again. On the other hand, if the adversary has not seen an image before, we fix a probability $\frac{N'}{N}$ that the adversary classifies the image as unknown.

We will compute the probability of successful classification for the adversary separately for images that are known and unknown to the user, which are:

$$\frac{N'}{N} + \left(1 - \frac{N'}{N}\right)^2 \text{ and } \frac{N'}{N} \text{ respectively.}$$

From these formulae, the adversary has at least 75% of success on each single image if $N'/N \geq 0.75$. We will denote this ratio as ε. We can estimate the expected number A of attempts by the adversary to know at least a proportion ε of the whole number N of images. This problem is related to the so-called *coupon collector's problem*. From the formula in [14, Section 2.1], we get:

$$A = N \sum_{i=\varepsilon N}^{N} \frac{1}{i} \sim N \ln\left(\frac{1}{1-\varepsilon}\right) \approx 1.39N.$$

We should then stop an adversary from obtaining too many images. If new images are added at every login, we get that N should quickly be in the hundreds. This means that a targeted attack would require many login attempts. This would get detected by the system which could create a lock-out. An alternative would be to increase $P(x)$ when many errors are detected and re-using old pictures, making brute-force easier but targeted attacks harder.

6.6 Constraint on a generalised use

To be sure that the protocol is scalable, having many different accounts with different services should not create any problem. One issue comes from the re-use of similar image databases. It is quite related to the problem of not showing the same pictures again by keeping track of which ones were seen, with the problem that there is no common database.

One improvement over the naive method of randomly selecting images is to select sets of 10 or 20 images. This lowers the probability of getting a familiar set, at the cost of obtaining all positives when a known set is used (in which case it is quite easy for the server to notice and cancel that set). Still, if all services apply this method with the same categorisation of images into sets, the probability of collision gets divided by 10.

This also means that less information has to be stored about which images have been seen. Depending on future empirical research on the performance of generated and composite images, a database of 10^{10} artificial images could be used naively for improved performance. This is just one of many potential improvements to the Reflexive Memory Authenticator, and we will now discuss a few other options.

7 Extensions and discussion

7.1 Potential extensions

Besides the potential optimisations already mentioned, we want to mention three ways to extend and improve this protocol. The first would be to reduce the

waiting time. This could be done by using loading times as an opportunity to show some images. The background images while the user waits or types their information could also be used as a way to create a baseline.

A second possibility would be to use this kind of protocol for continuous authentication, with an image being shown periodically, especially after extended pauses to make sure that the person using the device is the correct one. Such approaches would add security in the most critical times. As this interruption can be costly to the user, care has to be taken to ensure that it does not disrupt the workflow. This could be improved by using ideas from the field of considerate computing [45]. As such, the image challenges should not be shown while the user is typing, talking, making selections, or being presented with a complex decision or action. Instead, it would be better to challenge them as they are preparing to change task: closing a file or a tab, for example.

Finally, there is still a controversy about how much the brain really reacts to images shown for very brief durations (e.g. 30ms). An effect can be seen in certain cases, especially when it comes to pupil behaviour, where it can prime the user for faster reaction [19]. If that could be controlled, inserting test images within a short video could make a longer authentication process more bearable. However, this might bother some users conceptually, and it would require better models of pupil contraction.

This method could also be used in a more worrisome way, as it could allow an adversary to identify users without their knowledge or consent, by showing discreet images and studying their pupil reactions. It would be possible to counter this by making some mental computations, which affect pupil size, but this counter requires being aware that the test is ongoing. Even without going as far as identifying users, this pupil biometrics also have the potential to be used to expose the emotional state of the user — as well as whether they are intoxicated.

7.2 Testing reflexive pupil biometrics

One central outcome of this paper is that we need specific empirical studies on pupil sizes in memory effects, especially in the context of classification. Such efforts would not just improve the performance and understanding of the Reflexive Memory Authenticator, but also answer some fundamental questions. Many are still open:

- How fast can the system accurately discriminate between a familiar and a new image?
- What interactions need to be considered when using a resting period or when presenting many stimuli in a row, and can the interference be compensated?
- We currently try to get a single bit, but how much information can be reliably obtained by the dilation response? This could be done by allowing the classification to estimate the strength of recall instead of simply checking whether the image is familiar.
- How sensitive is the pupil reaction to the showing of pictures that are closely related to ones that are known or were recently shown?

– How is it affected by using synthetic or composite images?
– How usable would showing this stream of pictures be, and how would users react to it, especially in high frequencies? Could ocular fatigue be a problem?

References

1. Asghar, H.J., Li, S., Pieprzyk, J., Wang, H.: Cryptanalysis of the convex hull click human identification protocol. International Journal of Information Security **12**(2), 83–96 (2013)
2. Ashby, C., Bhatia, A., Tenore, F., Vogelstein, J.: Low-cost electroencephalogram (eeg) based authentication. In: 5th International IEEE/EMBS Conference on Neural Engineering – NER. pp. 442–445. IEEE (2011)
3. Bednarik, R., Kinnunen, T., Mihaila, A., Fränti, P.: Eye-movements as a biometric. In: Kalviainen, H., Parkkinen, J., Kaarna, A. (eds.) Image Analysis. pp. 780–789. Springer Berlin Heidelberg, Berlin, Heidelberg (2005)
4. Bowyer, K.W., Hollingsworth, K., Flynn, P.J.: Image understanding for iris biometrics: A survey. Computer Vision and Image Understanding **110**(2), 281–307 (May 2008)
5. Bradley, M.M., Lang, P.J.: Memory, emotion, and pupil diameter: Repetition of natural scenes. Psychophysiology **52**(9), 1186–1193 (2015)
6. Brostoff, S., Sasse, M.A.: Are passfaces more usable than passwords? a field trial investigation. In: McDonald, S., Waern, Y., Cockton, G. (eds.) People and Computers XIV — Usability or Else!: Proceedings of HCI. pp. 405–424. Springer London, London (2000)
7. Chiasson, S., Biddle, R., van Oorschot, P.C.: A second look at the usability of click-based graphical passwords. In: Proceedings of the 3rd Symposium on Usable Privacy and Security. pp. 1–12. SOUPS '07, ACM, New York, NY, USA (2007)
8. Choudhury, B., Then, P., Issac, B., Raman, V., Haldar, M.: A survey on biometrics and cancelable biometrics systems. International Journal of Image and Graphics **18** (01 2018)
9. Cody, S.: Do Only The Eyes Have It? Predicting Subsequent Memory with Simultaneous Neural and Pupillometry Data. Master's thesis, The Ohio State University (2015)
10. Curran, M.T., Yang, J.k., Merrill, N., Chuang, J.: Passthoughts authentication with low cost EarEEG. In: IEEE 38th Annual International Conference of the Engineering in Medicine and Biology Society – EMBC. pp. 1979–1982. IEEE (2016)
11. Das, R., Maiorana, E., Campisi, P.: Eeg biometrics using visual stimuli: A longitudinal study. IEEE Signal Processing Letters **23**(3), 341–345 (2016)
12. Deravi, F., Guness, S.P.: Gaze trajectory as a biometric modality. In: Biosignals. pp. 335–341 (2011)
13. Einhäuser, W.: The Pupil as Marker of Cognitive Processes, pp. 141–169. Springer Singapore, Singapore (2017)
14. Ferrante, M., Saltalamacchia, M.: The coupon collector's problem. Materials matemàtics pp. 0001–35 (2014)
15. Galdi, C., Nappi, M., Riccio, D., Cantoni, V., Porta, M.: A new gaze analysis based soft-biometric. In: Carrasco-Ochoa, J.A., Martínez-Trinidad, J.F., Rodríguez, J.S., di Baja, G.S. (eds.) Pattern Recognition. pp. 136–144. Springer Berlin Heidelberg, Berlin, Heidelberg (2013)

16. Galdi, C., Nappi, M., Riccio, D., Wechsler, H.: Eye movement analysis for human authentication: a critical survey. Pattern Recognition Letters **84**, 272–283 (2016)
17. German, R.L., Barber, K.S.: Consumer attitudes about biometric authentication. Tech. rep., University of Texas at Austin Center for Identity (2018)
18. Golla, M., Schnitzler, T., Dürmuth, M.: Will any password do? Exploring rate-limiting on the web. In: Who Are You ?! Adventures in Authentication (2016)
19. Gomes, C.A., Montaldi, D., Mayes, A.: The pupil as an indicator of unconscious memory: Introducing the pupil priming effect. Psychophysiology **52**(6), 754–769 (2015)
20. Jensen, W., Gavrila, S., Korolev, V., et al.: Picture password: A visual login technique for mobile devices. Tech. rep., National Institute of Standards and Technology (2003)
21. Just, M., Aspinall, D.: Personal choice and challenge questions: a security and usability assessment. In: Proceedings of the 5th Symposium on Usable Privacy and Security. p. 8. ACM (2009)
22. Just, M., Aspinall, D.: Challenging challenge questions: An experimental analysis of authentication technologies and user behaviour. Policy & Internet **2**(1), 99–115 (2010)
23. Kafkas, A., Montaldi, D.: Recognition memory strength is predicted by pupillary responses at encoding while fixation patterns distinguish recollection from familiarity. The Quarterly Journal of Experimental Psychology **64**(10), 1971–1989 (2011)
24. Karthika, S., Devaki, P.: An efficient user authentication using captcha and graphical passwords - a survey. International Journal of Science and Research p. 123 (2014)
25. Kasprowski, P., Komogortsev, O.V., Karpov, A.: First eye movement verification and identification competition at btas 2012. In: IEEE 5th International Conference on Biometrics: Theory, Applications and Systems – BTAS. pp. 195–202. IEEE (2012)
26. Klamkin, M.S., Newman, D.J.: Extensions of the birthday surprise. Journal of Combinatorial Theory **3**(3), 279–282 (1967)
27. Kollreider, K., Fronthaler, H., Bigun, J.: Evaluating liveness by face images and the structure tensor. In: IEEE 4th Workshop on Automatic Identification Advanced Technologies – AutoID. pp. 75–80 (Oct 2005)
28. Lashkari, A.H., Farmand, S., Zakaria, O.B., Saleh, R.: Shoulder surfing attack in graphical password authentication. International Journal of Computer Science and Information Security – IJCSIS **6**(2) (2009), http://arxiv.org/abs/0912.0951
29. Lee, C., Kim, J.: Cancelable fingerprint templates using minutiae-based bit-strings. Journal of network and computer applications **33**(3), 236–246 (2010)
30. de Leeuw, K.M.M., Bergstra, J.: The History of Information Security: A Comprehensive Handbook. Elsevier Science (2007)
31. Loftus, G.R.: Eye fixations and recognition memory for pictures. Cognitive Psychology **3**(4), 525–551 (1972)
32. Marcel, S., Millán, J.d.R.: Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. IEEE transactions on pattern analysis and machine intelligence **29**(4) (2007)
33. Moon, D., Yoo, J.H., Lee, M.K.: Improved cancelable fingerprint templates using minutiae-based functional transform. Security and Communication Networks **7**(10), 1543–1551 (Oct 2014). https://doi.org/10.1002/sec.788
34. N. Shepard, R.: Recognition memory for words, sentences, and pictures. Journal of Verbal Learning and Verbal Behavior **6**, 156–163 (02 1967). https://doi.org/10.1016/S0022-5371(67)80067-7

35. Naber, M., Frässle, S., Rutishauser, U., Einhäuser, W.: Pupil size signals novelty and predicts later retrieval success for declarative memories of natural scenes. Journal of vision **13**(2), 11–11 (2013)
36. Noton, D., Stark, L.: Scanpaths in saccadic eye movements while viewing and recognizing patterns. Vision Research **11**(9) (1971)
37. Phetmak, N., Liwlompaisan, W., Boonma, P.: Travel password: A secure and memorable password scheme. In: Nguyen, N.T., Attachoo, B., Trawiński, B., Somboonviwat, K. (eds.) Intelligent Information and Database Systems: 6th Asian Conference – ACIIDS. pp. 402–411. Springer International Publishing, Cham (2014)
38. Rajan, R., Selker, T., Lane, I.: Task load estimation and mediation using psychophysiological measures. In: Proceedings of the 21st International Conference on Intelligent User Interfaces. pp. 48–59. ACM (2016)
39. Rayner, K.: Eye movement latencies for parafoveally presented words. Bulletin of the Psychonomic Society **11**(1), 13–16 (1978)
40. Reddy, P.V., Kumar, A., Rahman, S., Mundra, T.S.: A new antispoofing approach for biometric devices. IEEE transactions on biomedical circuits and systems **2 4**, 328–37 (2008)
41. Rigas, I., Abdulin, E., Komogortsev, O.: Towards a multi-source fusion approach for eye movement-driven recognition. Information Fusion **32**, 13–25 (2016)
42. Roberts, C.: Biometric attack vectors and defences. Computers & Security **26**(1), 14–25 (2007)
43. Schechter, S., Brush, A.J.B., Egelman, S.: It's no secret. measuring the security and reliability of authentication via "secret" questions. In: 30th IEEE Symposium on Security and Privacy. pp. 375–390. IEEE (2009)
44. Segreti, S.M., Melicher, W., Komanduri, S., Melicher, D., Shay, R., Ur, B., Bauer, L., Christin, N., Cranor, L.F., Mazurek, M.L.: Diversify to survive: Making passwords stronger with adaptive policies. In: 13th Symposium on Usable Privacy and Security – SOUPS. pp. 1–12. USENIX Association, Santa Clara, CA (2017)
45. Selker, T.: Understanding considerate systems — UCS (pronounced: You see us). In: 2010 International Symposium on Collaborative Technologies and Systems. pp. 1–12 (May 2010). https://doi.org/10.1109/CTS.2010.5478532
46. Singh, S., Agarwal, G.: Integration of sound signature in graphical password authentication system. International Journal of Computer Applications **12**(9), 11–13 (2011)
47. Sluganovic, I., Roeschlin, M., Rasmussen, K.B., Martinovic, I.: Using reflexive eye movements for fast challenge-response authentication. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. pp. 1056–1067. CCS '16, ACM, New York, NY, USA (2016)
48. Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A., Memon, N.: Passpoints: Design and longitudinal evaluation of a graphical password system. International journal of human-computer studies **63**(1-2), 102–127 (2005)
49. Zviran, M., Haga, W.J.: Cognitive passwords: The key to easy access control. Computers & Security **9**(8), 723–736 (1990)