Reflexive Memory Authenticator: A proposal for effortless renewable biometrics

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

[1]Digitrust, Loria, Université de Lorraine, www.koliaza.com

[2]Université Côte d'Azur, INRIA Sophia-Antipolis, France

[3]University of Maryland, Baltimore County

2nd International Workshop on Emerging Technologies for Authorization and Authentication
@ ESORICS September 27th, 2019

An issue with biometrics

The *state space is too small* for current accuracies:

- Static biometrics don't get better than 0.01% EER
- Behavioural biometrics often are above 1% EER

For static biometrics, *unchangeability* is a big issue

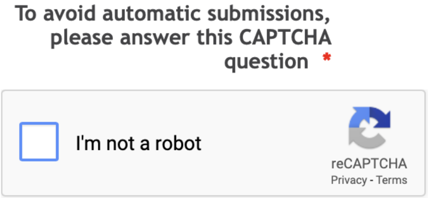
- Replay attacks
- Phishing is viable
- Modelisation when replay is not available

Despite little guarantees, more problems from high public trust. Leaks become possible.

Challenge systems

Many challenge systems:

- Text challenges (personal questions)
- Graphic passwords
- CAPTCHAs



To avoid automatic submissions, please answer this CAPTCHA question *

□ I'm not a robot

Common problems:

- Either slow or unsecure
- Limited usability and requires user effort
- Vulnerable to shoulder-surfing and targeted attacks
- Hard to create good challenges

Biometric challenges

Only two real types of challenge biometric systems have been considered:

- Electro-encephalography
- Eye movement biometrics with arbitrary patterns

Problems:

- High EER
- Based on modelising hidden variables instead of challenges themselves

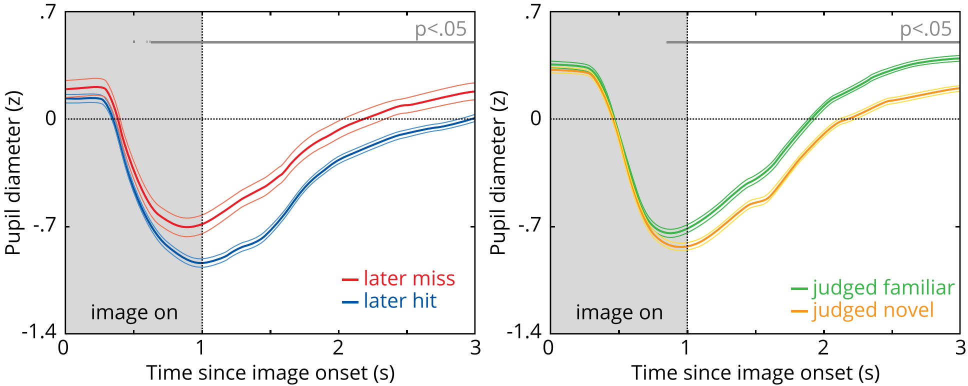
The pupil memory reflex

When seeing an image, the pupil contracts then dilates before getting back to normal.

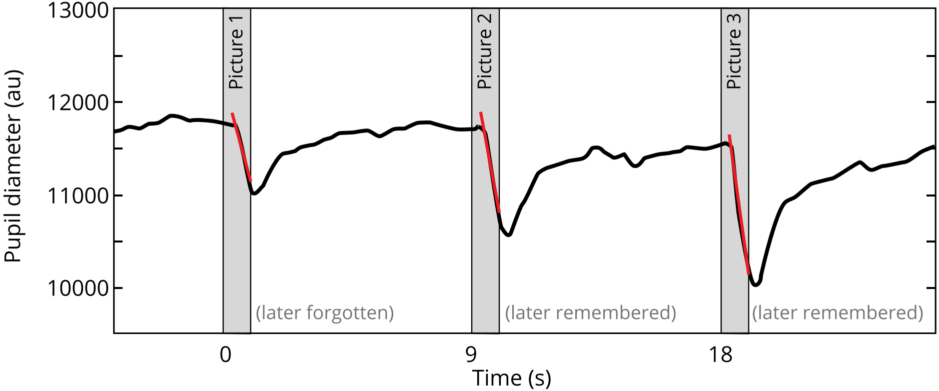
Contraction and dilation speed and magnitude depend on the familiarity of the image.

Many experiments since 1967, some organised recently by Naber, Frässle, Rutishauser, and Einhäuser (2013), and Bradley and Lang (2015).

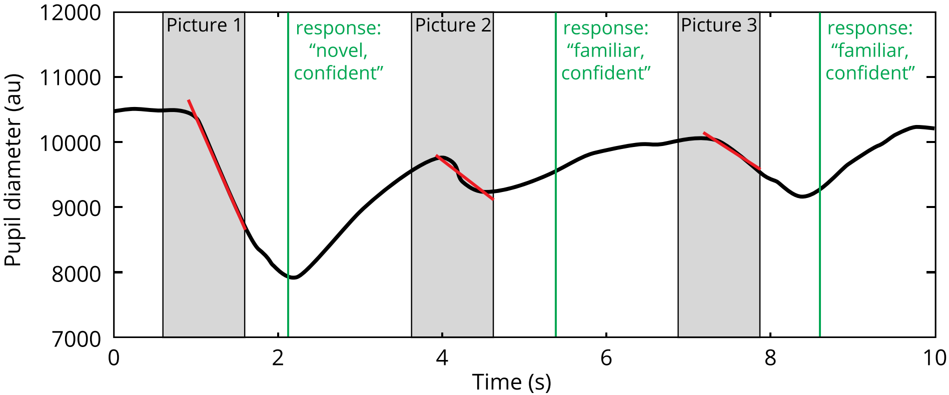
The pupil memory reflex: speed (Naber et al.)



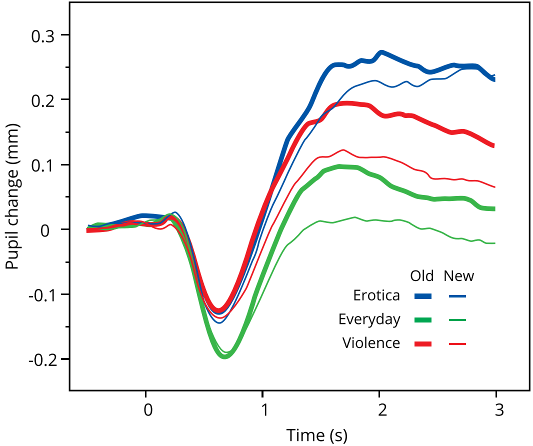
The pupil memory reflex: repeated tests, memorisation (Naber et al.)



The pupil memory reflex: repeated tests, retrieval (Naber et al.)



The pupil memory reflex: emotional content (Bradley and Lang)



High-level protocol

At account creation, memorise ≈ 30 randomly selected pictures.

Authentication protocol:

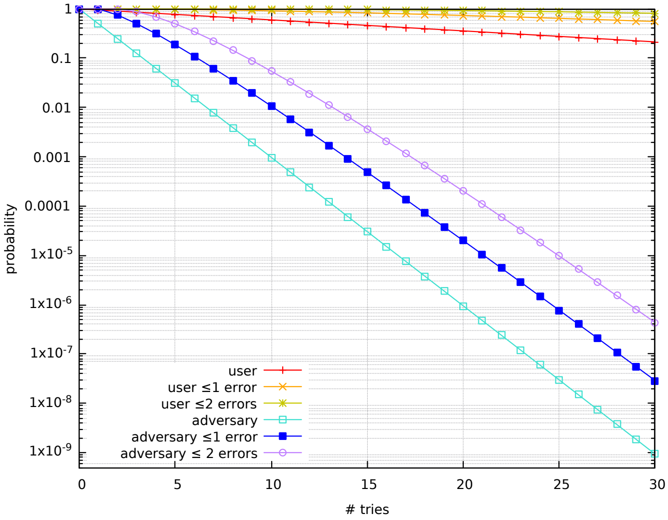
1. Show a picture randomly selected from the known or unknown sets;
2. Detect pupil size variation;
3. Categorise the reaction as known or unknown;
4. Update probability of being user/intruder
5. Accept or trigger alarm

Protocol parameters

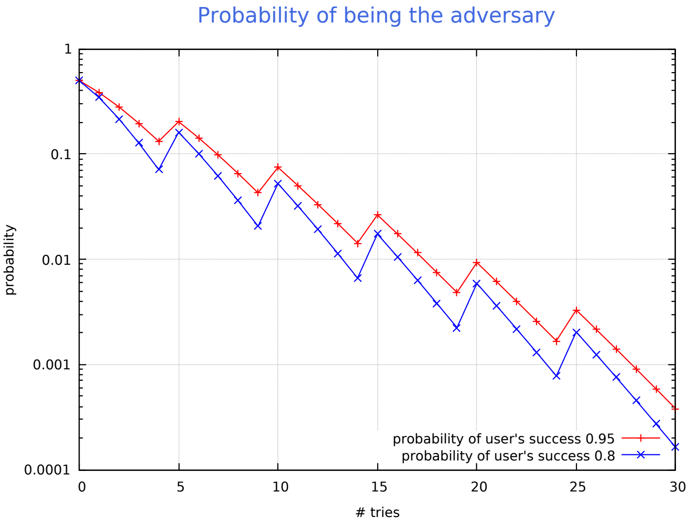
Many parameters to determine

- Image types and sources
- Relative probability of known/unknown images
- Time per image and resting period
- Threshold for acceptance/rejection/continued testing

RMA success rate ($p_{x_0} = p_{y_1} = 0.95$)



Adaptive probability of being the user



Implementation considerations

Some algorithmic questions:

- How to handle noise cancellation?
- How to keep track of the images shown?
- How to prevent targeted attacks?
- What happens if used for many services?

Potential extensions

Three potential improvements/extensions:

- Use loading times to show a standard image for a baseline
- Create continuous authentication, following considerate computing principles
- Potential non-noticeable use to detect intoxication/modified mental states

Future work and open problems

We raise multiple questions:

- How fast can we discriminate between known/unknown images?
- Can we compensate the interference without a rest period?
- Can we get more than 1 bit of data?
- How do we react to image closely related to known ones? To composite images?
- What happens if we show a high frequency stream? A long stream?
- Can ocular fatigue become a problem?

Thank you for your attention