Visual Secrets : A recognition-based security primitive and its use for boardroom voting

Enka Blanchard
CNRS
LAMIH, Université Polytechnique Hauts-de-France, Valenciennes
Center for Internet and Society, Paris, France

Sébastien Bouchard
Sorbonne Université, CNRS, LIP6, F-75005 Paris, France

Ted Selker,
Cyber Defense Lab
University of Maryland, Baltimore County (UMBC), USA

Abstract. This paper presents and evaluates a new security primitive in the form of non-transferable "visual secrets". We show how they can be used in the design of voting systems. More specifically, we introduce a receipt-free low-tech visually verifiable boardroom voting system which is built for simplicity and can serve as a teaching tool to introduce people to verifiable voting.

Keywords: Usable security, Boardroom voting, Verifiability, User studies, Cognitive psychology

1 Introduction : defining visual secrets

After 20 years of advances in verifiable voting, there is still limited understanding by the public of both how verification works, and why voting systems should be verifiable [3]. Besides, the usability costs remain high, both for end-users and administrators, limiting the number of users who verify their votes [12]. We initially sought to improve usability by simplifying verification based on long vote-codes, and instead found a new security primitive that could have multiple applications, including as the central component of a simple voting system meant to introduce users to the concept of verifiable voting.

Most secrets employed in usable security are shareable : one can give their home keys to a friend, be coerced into revealing passwords, or even have their biometrics such as fingerprints stolen [9]. One natural question is then to ask whether it is possible for humans to have (useful) secrets that cannot be shared ? In a formal way, the answer seems to be no, but if we set reasonable constraints, some tentative solutions can be found.

Our lead is to use specialised human cognitive functions and in particular image recognition. As has been demonstrated since the 1960s, humans have an

extensive memory for visual stimuli [6]. A significant aspect of this image recognition happens in a pre-semantic and pre-cognitive fashion, requiring no conscious effort, thanks to specialised neural pathways in multiple areas of the brain [10, 6]. This is related to the difference between recognition and recall [5]. The mind's pre-semantic treatment means that there might be a loss of information during image recognition. The ability to recognise an image is not directly related to our mental description of it, and any description might ignore some key elements of the picture. This pre-semantic treatment is used as a source of secrets that are recognisable but not shareable, and we call the resulting primitive a *visual secret*.

A user with unlimited time and good eyesight might be able to describe exhaustively each pixel of an image. However, practical protocols would have reasonable constraints on the time spent describing images. These constraints are especially appropriate in our case, as the first proposed application of visual secrets concerns verifiable voting in a boardroom setting. This corresponds to a small group of participants — e.g., jury members — having to quickly vote on an issue, generally between two possibilities.

2 Empirical study

The goal of the study was to test the viability of visual secrets as a security primitive. Subjects were shown three pictures and had to describe them, before having to find their initial pictures among two sets of 10 similar pictures in random order. For the three series, we settled on public domain images of animal faces (lions), natural scenes (mountains), and abstract images, as we conjectured that the latter would be harder to describe. We recruited 164 volunteers through John Krantz's Psychological Research on the Net index [7]. We eliminated subjects who had not provided intelligible answers when asked to describe pictures, leaving 151 subjects.

Subjects could recognise their pictures with high reliability (83%, 86% and 79% for the lions, mountains and abstracts pictures respectively). When compared to a null hypothesis of 5% (for optimised random choice), this is highly significant (z-scores >40 for all series, corresponding to p-values $< 10^{-350}$).

To estimate image describability, two of the authors independently categorised the full list of descriptions subjects wrote about their assigned images. For each description, the assessors selected all images that could potentially fit — without knowing what the correct answer was.

To assess the security of the images as potential visual secrets, one question is crucial : can they be accurately and unambiguously de-

	Assessor	Lion	Mountain	Abstract
Correctly unambiguous	Strict	36	40	35
	Lenient	32	23	7
Wrongly unambiguous	Strict	17	16	16
	Lenient	8	5	3
Unambiguous accuracy	Strict	68%	71%	69%
	Lenient	80%	82%	70%

scribed, or in other words, does a description fits a single image ? The adjoining table shows for each image series and assessor the number of descriptions thought to be unambiguous, how many of those were in fact attributed to the wrong image, and the accuracy. The proportion of unambiguous descriptions was at most 37%, and those descriptions were wrongly attributed in 18-32% of cases. A coercer trying to obtain the secret would then have succeeded in at most 26% of cases, with an additional 8% of cases where they would have been (wrongly) sure that they had found the correct secret. We've thus established that visual secrets are close to our objectives: highly recognisable (79-86%) but poorly describable.

3 Visually Verifiable Ballots (VVB)

We now describe a first application of visual secrets in the form of a low-tech — in our case, paper — voting system appropriate for boardroom elections. VVB are meant to be low-tech system that is not subject to the attacks mentioned in [2] and a cheap teaching tool that is easy to use and can introduce users to the concepts of verifiable voting (before moving on to more secure and complex systems such as Belenios [4]).

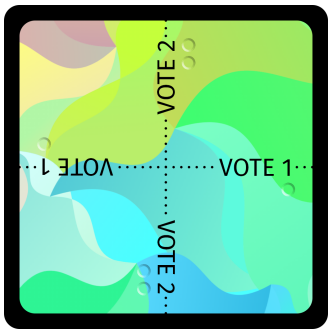

Fig. 1. Example of a Visually Verifiable Ballot.

Visually Verifiable Ballots look and feel like square cards (shown on Figure 1). One side is left blank — or with a regular symmetrical pattern — and the other has the relevant information : a picture from a common set of visual secrets, covering the whole card, and two orthogonal lines crossing the picture, labelled "Vote 1" and "Vote 2". This visual information is complemented by tactile information in the form of texture — bumps — present on both ends of each line, with one bump for the first and two for the second. The protocol goes as follows :

1. The vote organiser opens a new pack of ballots in front of all voters ;
2. One ballot is distributed face down to each voter ;
3. Each voter lifts up their ballot to look at the image and memorise it ;
4. Each voter rotates their ballot a few times, keeping track of its orientation ;
5. Each voter folds their ballot along the line of their choice to select "Vote 1" or "Vote 2" to be on the inside fold, without marking or modifying their ballot in any other way ;
6. The voters cast their ballots in a ballot box or a bag ;
7. The ballot box is upturned and all the ballots are unfolded on a table in front of all the voters' eyes ;
8. The vote organiser tallies the votes orally while the voters check that the ballot featuring their assigned picture are present with the correct fold ;
9. If a voter sees their ballot folded the wrong way or cannot find their ballot, they announce as much without giving any additional information ;
10. The vote organiser announces the result and the vote is over unless someone challenges the result.

4 Concluding remarks

This paper introduced a security primitive called visual secrets, a kind of non-shareable secret that is pure information and does not depend on possessing an item. Its strength comes from the following two properties of pictures. They are highly recognisable, with subjects having 80%+ chance of recognising their own secret. It is difficult to unambiguously describe them. No assessor managed to get better than 82% accuracy on the 15-25% of descriptions which they thought were unambiguous. This primitive shows that cognitive responses can be used to design or improve low-tech voting protocols, and we propose one such protocol for boardroom voting. Visual secrets could also be used as a replacement for the identifying marks used in other verifiable voting systems such as sElect [8] or protocols inspired by Ron Rivest's ThreeBallot [11, 1].

A longer version of this paper and the data files for the experiment are available at `https://hal.archives-ouvertes.fr/hal-03133412`.

References

1. Blanchard, E., Selker, T.: Origami voting: a non-cryptographic approach to transparent ballot verification. In: 5th Workshop on Advances in Secure Electronic Voting (2020)
2. Blanchard, E., Selker, T., Sherman, A.T.: Boardroom voting: Practical verifiable voting with ballot privacy using low-tech cryptography in a single room (2019), https://hal.archives-ouvertes.fr/hal-02908421/
3. Burton, C., Culnane, C., Schneider, S.: vvote: Verifiable electronic voting in practice. IEEE Security & Privacy **14**(4), 64–73 (2016)
4. Cortier, V., Gaudry, P., Glondu, S.: Belenios: a simple private and verifiable electronic voting system. In: Foundations of Security, Protocols, and Equational Reasoning, pp. 214–238. Springer (2019)
5. Haist, F., Shimamura, A.P., Squire, L.R.: On the relationship between recall and recognition memory. Journal of Experimental Psychology: Learning, Memory, and Cognition **18**(4), 691 (1992)
6. 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)
7. Krantz, J.H.: Psychological research on the net (2019), `https://psych.hanover.edu/research/exponnet.html`
8. Küsters, R., Müller, J., Scapin, E., Truderung, T.: select: A lightweight verifiable remote voting system. In: 2016 IEEE 29th Computer Security Foundations Symposium (CSF). pp. 341–354 (2016). https://doi.org/10.1109/CSF.2016.31
9. Li, S., Kot, A.C.: Attack using reconstructed fingerprint. In: IEEE International Workshop on Information Forensics and Security – WIFS. pp. 1–6. IEEE (2011)
10. 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)
11. Rivest, R.L., Smith, W.D.: Three voting protocols: Threeballot, vav, and twin. In: Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology. pp. 16–16. EVT'07, USENIX Association, Berkeley, CA, USA (2007)
12. Solvak, M.: Does vote verification work: Usage and impact of confidence building technology in internet voting. In: International Joint Conference on Electronic Voting. pp. 213–228. Springer (2020)