TAPCHA – An 'Invisible' CAPTCHA Scheme

Nan Jiang
Bournemouth University
Fern Barrow, Poole BH12 5BB
njiang@bournemouth.ac.uk

Huseyin Dogan
Bournemouth University
Fern Barrow, Poole BH12 5BB
hdogan@bournemouth.ac.uk

TAPCHA is a universal CAPTCHA scheme designed for touch-enabled smart devices such as smartphones, tablets and smartwatches. The main difference between TAPCHA and other CAPTCHA schemes is that TAPCHA retains its security by making the CAPTCHA test 'invisible' for the bot. It then utilises context effects to maintain the readability of the instruction for human users which eventually guarantees the usability of the scheme. Two reference designs, namely TAPCHA SHAPE & SHADE and TAPCHA MULTI are developed to demonstrate the use of this scheme.

CAPTCHAs. Smart devices. Smartphones. TAPCHA. Usability. Security. Context effect.

1. INTRODUCTION

CAPTCHAs (Completely Automated Public Turing Test to Tell Computers and Humans Apart) are a popular security mechanism used to make sure only human users are able to use the protected online services not the bots. They are considered as a type of challenge-response authentications where human interactive proofs (HIPs) are needed for distinguishing humans and computers (Chew & Baird 2003, Chellapilla et al. 2005).

Current mainstream CAPTCHAs are text-based CAPTCHAs. In these schemes, online users are often required to recognise distorted characters presented in an image or video clip. However, in order to maintain sufficient security level, recognising distorted characters successfully has become increasingly difficult (Yan et al. 2008, Bursztein et al. 2010). This gets even worse on mobile devices due to the limited display size and the shift of using keyboards to touch gestures (Lin et al. 2011, Shirali-Shahreza et al. 2013, Wismer et al. 2012).

New interactive CAPTCHA schemes have been proposed to tackle these challenges on mobile devices such as µcaptcha (Leiva & Alvaro 2015) and What's up CAPTCHA (Gossweiler et al. 2009). These schemes rely on identifying appropriate challenges and required interactions which are human friendly and bot resistant.

In this paper, we present TAPCHA, a universal CAPTCHA scheme where its security is retained through making the challenges 'undiscoverable' from a bot. Unlike the existing ones which focus on making the challenges 'hard to complete' yet 'discoverable' by the bots, our scheme provides flexibility in designing the challenges and deciding the interaction methods. We achieve this by processing the challenge description similar methods seen in present text-based CAPTCHAs to make it hard for a bot to recognise and understand.

2. HOW TO 'HIDE' CHALLENGE DESCRIPTION

Consider some attempts to make text-based CAPTCHAs more secure (Alsuhibany 2011, Baird & Riopka 2005, Bursztein et al. 2011, El Ahmad et al. 2012). Similar approaches can be taken to make the challenge description hard to be recognised by a bot. Unlike computer bots, human users can benefit from the context effects (McClelland & Rumelhart 1981). This means as long as adequate information cues are present within the whole challenge (description and presentation), human users can still figure out what the challenge is about. Figure 1 shows an example where most words in the challenge description are distorted such as "move", "from", "left", "touch" and "is" etc. When more contexts are given, the challenge will become more understandable by human users.

The benefits are obvious. First, it provides flexibility in designing challenges and deciding suitable interaction methods for the end devices without limiting itself to certain types of challenges and interaction methods. For example, a test could be moving specific objects around, tapping specific objects in order or even drawing a specific shape on the screen. Second, although the security of the scheme is mainly retained through the processed challenge description, it can be further reinforced through the challenge itself. For example, in an object moving challenge, more objects and subtests can be introduced to further reduce the mathematical probability to compromise the challenge without significantly increase the complexity of the test.

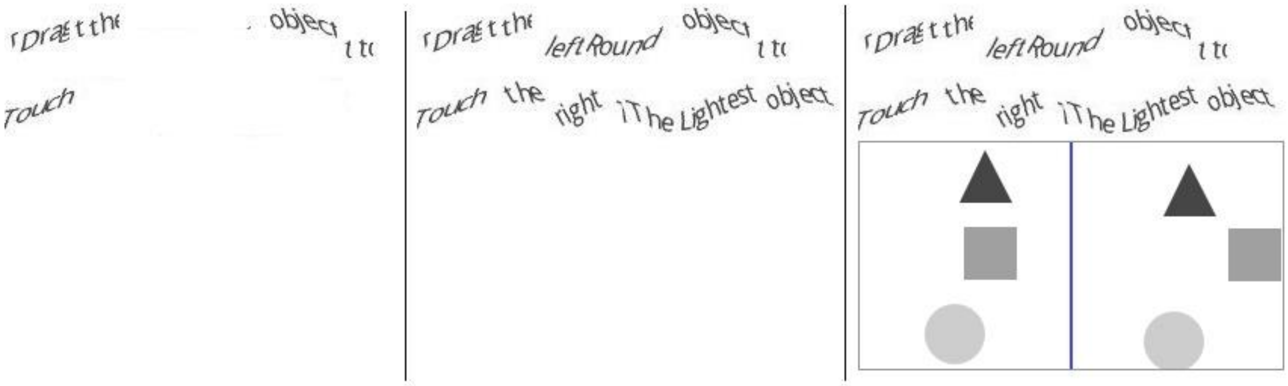


Figure 1: *Processed instruction with different levels of context provided (left: no context, middle: context level 1, right: context level 2)*

3. TAPCHA SHAPE & SHADE

3.1 Design

TAPCHA Shape & Shade features ‘swipe’ based challenges that ask the user to move a specific object from the left side of the canvas to touch another specific object on the right side of the canvas. The specificity of the object is determined by its shape and/or shade. The challenge description is mainly processed by using high strength waveform transformation with anti-bot segmentation adjustment. Figure 2 shows an example where a user is required to move the lightest object from the left (i.e., round) to touch the triangle on the right.

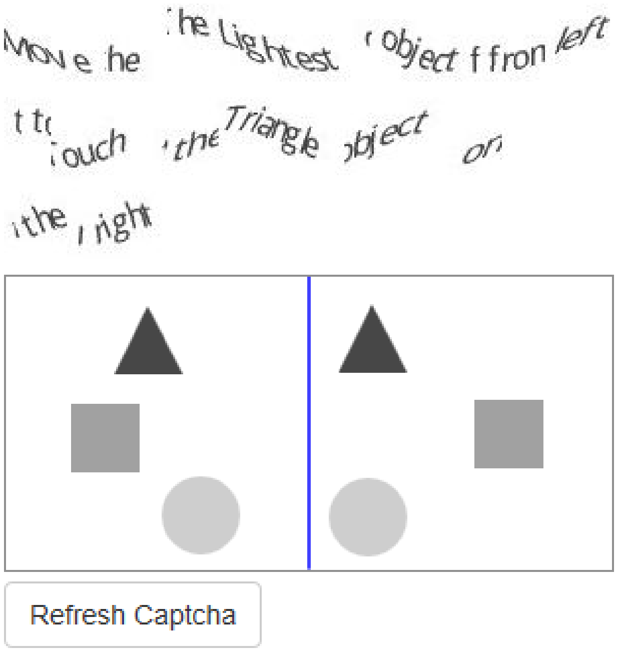


Figure 2: *TAPCHA Shape & Shade demonstration*

For added security, the challenge description features randomly generated keywords with similar meanings and random sentence structures using the following construction:

Action {1…n}, (Direction) (Specificity) Object | *Object (Specificity) (Direction), Action {a…z}, (Direction) (Specificity) Object* | *Object (Specificity) (Direction).*

For example, the same challenge could be given a description of “Move the square object from left to touch the right object which is the lightest” or “Drag the left square object to touch the right round object”.

3.2 Security

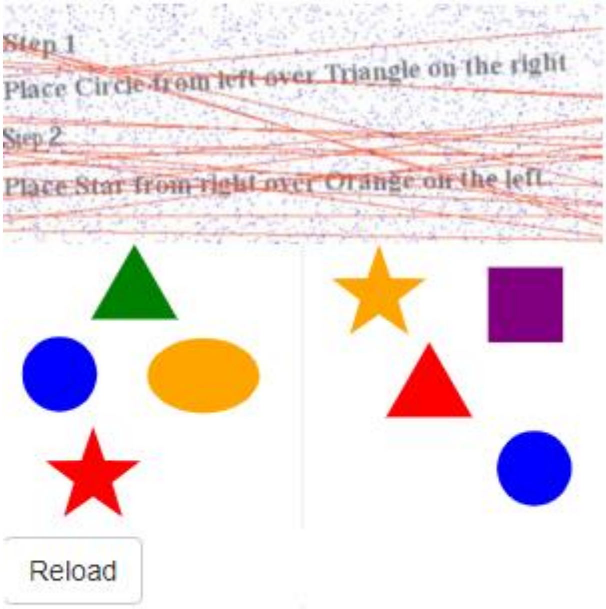
The mathematical probability to compromise TAPCHA Shape & Shade is determined by the number of objects presented in the test. Taking the example shown in Figure 2, the probability will be 1/(6*5) = 3.33% (Jiang & Dogan 2015).

The OCR test on the challenge description using Google Cloud Vision API shows the average success rate of instruction text recognition is: 23.5%.

4. TAPCHA MULTI

4.1 Design

TAPCHA Multi features similar swipe based challenges to TAPCHA Shape & Shade. The differences are: (1) the specificity of objects is now determined by its shape and colour and (2) the user needs to swipe more than once based on the challenge description. Figure 3 shows an example where a user is asked to (1) place the round object from the left over the triangle on the right and (2) place the star from the right over the orange object on the left.



Step 1
Place Circle from left over Triangle on the right
Step 2
Place Star from right over Orange on the left

Figure 3: *TAPCHA Multi demonstration*

4.2 Security

The mathematical probability to compromise TAPCHA Multi is determined by the number of objects presented in the test. Taking the example shown in Figure 3, the probability will be 1/(8x7)^2 = 0.03%.

5. CONCLUSION

In this paper, we presented TAPCHA, a universal CAPTCHA scheme designed for touch enabled smart devices including smartphones, tablets and smartbands. TAPCHA is different from other approaches as it tries to 'hide' a challenge from computer bots by processing the challenge description to make it unrecognisable by them. This is achieved through using similar methods noted in some text based CAPTCHA schemes. At the same time, as human users can benefit from the context effects, with adequate information cues presented within the whole challenge, they can still understand the challenge and complete it. The benefit is twofold. First, it provides flexibility in designing challenges and deciding suitable interaction methods for the end devices. Second, although the security of TAPCHA is mainly retained through the processed challenge description, it can be further reinforced through the challenge itself. To demonstrate how TAPCHA can be used in real world, TAPCHA Shape & Shade and TAPCHA Multi are developed. Our next step is to test TAPCHA using the two demos developed with real users to further understand its usability.

6. REFERENCES

Alsuhibany, S.A. (2011) Optimising CAPTCHA generation. In: the 2011 6th International Conference on Availability, Reliability and Security (ARES '11), Vienna, Austria, 22-26 August, pp. 740-745. IEEE Computer Society, Washington, DC, USA.

Baird, H.S., Riopka, T.P. (2005) ScatterType: a reading CAPTCHA resistant to segmentation attack. In: SPIE Document Recognition & Retrieval XII, San Jose, CA, USA, 16-20 January, 5676. Society of Photo Optical, USA.

Bursztein, E., Bethard, S., Fabry, C., Mitchell, J.C. and Jurafsky, D. (2010) How good are humans at solving CAPTCHAs? A large scale evaluation. In: the 2010 IEEE Symposium on Security and Privacy (SP '10), Oakland, CA, USA, 16-19 May, pp. 399-413. IEEE Computer Society, Washington, DC, USA.

Bursztein, E., Martin, M. and Mitchell, J. (2011) Text-based CAPTCHA strengths and weaknesses. In: the 18th ACM Conference on Computer and Communications Security (CCS '11), Chicago, IL, USA, October 17-21 October, pp. 125-138. ACM, New York, NY, USA.

Chellapilla, K., Larson, K., Simard, P. and Czerwinski., M. (2005) Designing human friendly human interaction proofs (HIPs). In: the 2005 SIGCHI Conference on Human Factors in Computing Systems (CHI '05), Portland, OR, USA, 2-7 April, pp. 711-720. ACM, New York, NY, USA.

Chew, M., Baird, H.S. (2003) Baffletext: A human interactive proof. In: SPIE Document Recognition & Retrieval X, Santa Clara, CA, USA, 20-24 January, 5010, pp. 305-316. Society of Photo Optical, USA.

El Ahmad, A.S., Yan, J. and Ng, W.Y. (2012) CAPTCHA Design: Color, Usability, and Security. Internet Computing, 16(2), pp. 44-51.

Jiang, N. and Dogan, H. (2015) A gesture-based CAPTCHA design supporting mobile devices. In: 2015 British Human Computer Interaction Conference (British HCI), Lincoln, UK, 15-17 July, pp. 202-207. ACM, New York, NY, USA.

Leiva, L. A., Alvaro, F. (2015) µcaptcha: Human Interaction Proofs tailored to touch-capable devices via math handwriting. International Journal of Human-Computer Interaction, 31(7), 457-471.

Lin, R., Huang, S., Bell, G.B. and Lee, Y. (2011) A new CAPTCHA interface design for mobile devices. In: the 12th Australasian User Interface Conference (AUIC '11), Perth, Australia, 17 – 20 January, vol 117, pp. 3-8. Australian Computer Society, Inc., Darlinghurst, Australia.

McClelland, J. L., Rumelhart, D.E. (1981) An interactive activation model of context effects in letter perception: I. An account of basic findings. Psychological review, 88(5), pp. 375.

Shirali-Shahreza, S., Penn, G., Balakrishnan, R. and Ganjali, Y. (2013) Seesay and hearsay captcha for mobile interaction. In: the 2013 SIGCHI Conference on Human Factors in Computing Systems (CHI '13), Paris, France, 27 April - 2 May, pp. 2147-2156. ACM, New York, NY, USA.

Wismer, A.J., Madathil, K.C., Koikkara, R., Juang, K.A. and Greenstein, J.S. (2012) Evaluating the usability of CAPTCHAs on a mobile device with voice and touch input. In: the 56th Human Factors and Ergonomics Society Annual Meeting, Boston, MA, USA, 22-26 October, 56(1), pp. 1228-1232. Sage, Los Angeles, CA, USA.

Yan, J., El Ahmad, A. S. (2008) Usability of CAPTCHAs or usability issues in CAPTCHA design. In: the 4th Symposium on Usable Privacy and Security (SOUPS' 08), Pittsburgh, PA, USA, 23-25 July, pp. 44-52. ACM, New York.