2017

Text-based CAPTCHAs over the years

Yang-Wai Chow
University of Wollongong, caseyc@uow.edu.au

Willy Susilo
University of Wollongong, wsusilo@uow.edu.au

Text-based CAPTCHAs over the years

Abstract

The notion of CAPTCHAs has been around for more than two decades. Since its introduction, CAPTCHAs have now become a ubiquitous part of the Internet. Over the years, research on various aspects of CAPTCHAs has evolved and different design principles have emerged. This article discusses text-based CAPTCHAs in terms of their fundamental requirements, namely, security and usability. Practicality necessitates that humans must be able to correctly solve CAPTCHA challenges, while at the same time automated computer programs should have difficulty solving the challenges. This article also presents alternative paradigms to text-based CAPTCHA design that have been examined in previous work. With the advances in techniques to defeat CAPTCHAs, the future of auto- mated Turing tests is an open question.

Disciplines

Engineering | Science and Technology Studies

Publication Details

Chow, Y. & Susilo, W. (2017). Text-based CAPTCHAs over the years. IOP Conference Series: Materials Science and Engineering, Vol 273 (pp. 1-6). United States: IOP Publishing.

Text-based CAPTCHAs over the years

IOP Conf. Series: Materials Science and Engineering **273** (2017) 012001 doi:10.1088/1757-899X/273/1/012001

Text-based CAPTCHAs over the years

Y W Chow and W Susilo

Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, University of Wollongong, Australia

E-mail: wsusilo@uow.edu.au

Abstract. The notion of CAPTCHAs has been around for more than two decades. Since its introduction, CAPTCHAs have now become a ubiquitous part of the Internet. Over the years, research on various aspects of CAPTCHAs has evolved and different design principles have emerged. This article discusses text-based CAPTCHAs in terms of their fundamental requirements, namely, security and usability. Practicality necessitates that humans must be able to correctly solve CAPTCHA challenges, while at the same time automated computer programs should have difficulty solving the challenges. This article also presents alternative paradigms to text-based CAPTCHA design that have been examined in previous work. With the advances in techniques to defeat CAPTCHAs, the future of auto- mated Turing tests is an open question.

Keywords: CAPTCHA, security, Turing test, usability

1. Introduction

The term CAPTCHA is an acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart" and was coined by von Ahn et al. [1] in their seminal paper on proposing the challenge of using hard Artificial Intelligence (AI) problems for security. CAPTCHAs refer to automated challenge-response tests that humans can pass, but current computer programs cannot pass [1]. Before the introduction of the term CAPTCHA, the notion of "automated Turing tests" was previously proposed by Naor [2] in an unpublished manuscript. Furthermore, CAPTCHAs have also been referred to in other work as "Human Interaction Proofs" (HIPs) [3, 4].

These days, CAPTCHAs are a common part of the Internet and are used on various websites to distinguish whether an online service is legitimately being used by a human, or being accessed by a computer program (otherwise known as a "bot"). Its use has been effective, to a certain extent, in deterring the automated abuse of online services intended for humans [5]. As examples, CAPTCHAs have been effective in preventing malicious bot programs from signing up for thousands of free email accounts and in deterring bots from sending out thousands of spam messages every minute [6].

Numerous CAPTCHA schemes have emerged over the years. The reason for this is because many schemes have been found to be vulnerable to automated attacks, and practitioners have attempted to design more robust schemes. In addition, there has been much research on examining various CAPTCHA schemes for design flaws and weakness that can be exploited to defeat the overall scheme [6–12]. This highlights the challenging and daunting task of developing a good scheme that is robust against auto- mated attacks. To further complicate matters, not only must a good CAPTCHA be secure against attacks, it must also be easily usable by humans. It would defeat the underlying purpose of a CAPTCHA if a human had difficulty in correctly solving a challenge generated from such a scheme.

To date, there are a variety of different CAPTCHA categories and approaches. To illustrate its diversity, different approaches in CAPTCHA schemes include text-based, image-based, audio-based,

containing animation, game-based requiring interaction, and so on. This article mainly focuses on text-based CAPTCHAs, which have been the most predominant form since its inception. Text-based CAPTCHAs generally consist of a sequence of alphanumeric characters, which can easily be entered via a keyboard, that are presented in the form of an image. The image may contain some sort of visual noise (e.g., a textured background) and the characters are typically distorted to impede recognition by automated computer attacks. The widespread popularity of the text-based approach is due to its intuitiveness from a human usage point of view, as well as its low implementation cost in terms of being able to automatically generated different challenges easily and present this to the user without requiring much computational resources [13].

This article discusses research on text-based CAPTCHAs, and how this has progressed and evolved over the years. It presents the fundamental design issues, namely, security and usability, along with the various forms of text-based CAPTCHAs that have been proposed by researchers and practitioners as alternatives to the traditional form of CAPTCHAs. In addition, this article also presents research on methods for defeating such CAPTCHAs.

2. Design issues

The security and usability of a resulting CAPTCHA are two of the main issues that must be considered in the design of a scheme. Security refers to the robustness of a scheme against automated attacks by a computer program, whereas usability refers to the ease at which a human can correctly solve the challenges.

The tradeoff between CAPTCHA security and usability is a difficult act to balance. This is because any practical scheme necessitates that humans must be able to correctly solve the challenges with a high success rate, while at the same time the probability that a computer program can correctly solve it must be very small. It has been stated that the design of a robust CAPTCHA must somehow capitalize on the difference in ability between humans and current computer programs [5]. With advances in research areas like computer vision and machine learning, it is debatable whether or not it is possible to design a CAPTCHA that is easy for humans but difficult for computer programs, and as such this remains an open question.

2.1. Security

Over the years, CAPTCHA security has been the topic of much research. Early work on the security of CAPTCHAs by Mori and Malik [7] showed that automated computer programs were capable of solving text-based CAPTCHAs at high success rates. In their work, they demonstrated a method of solving CAPTCHAs based on matching shape contexts of characters based on an image database of known objects, even in the midst of severe visual clutter. Their work highlighted the fact that with knowledge of a scheme's font and lexicon, CAPTCHAs based on language models are susceptible to dictionary attacks. Research also showed that distorted objects could be recognized using distortion estimation and removal techniques [8].

In other pioneering work, Chellapilla et al. [4] showed that machine learning algorithms were capable of breaking a variety of CAPTCHA schemes, without having to rely on language models. In their work, they proposed that solving a text-based CAPTCHA challenge consists of two main stages: segmentation and recognition. Segmentation refers to finding the locations of characters, whereas recognition is the identification of the characters. Their work demonstrated that the recognition problem is a trivial task for machine learning algorithms. This in turn led to the widely accepted segmentation- resistant principle for text-based CAPTCHA design, which states that if a CAPTCHA can be segmented into its constituting characters, it is essentially broken.

In later work examining the strengths and weaknesses of text-based CAPTCHAs, it was observed

that the segmentation-resistant principle alone is not enough to guarantee that a CAPTCHA scheme is secure against automated attacks [10]. In fact, Google's popular "reCAPTCHA", which was text-based at the time and designed to be segmentation- resistant, was successfully broken using a holistic approach of recognizing shape con- texts of entire words [14] and also in an approach using heuristic character segmentation and recognition [15].

2.2. Usability

Practicality dictates that ease of use for a human is another fundamental requirement of CAPTCHAs. However, this requirement often conflicts with the security requirement. For example, as previously discussed, CAPTCHAs based on language models are susceptible to attacks due to a readily available dictionary of words. Nevertheless, research has shown that humans find familiar text, like dictionary words, easier to read as opposed to unfamiliar text [16]. As such, a potential compromise is to adopt the use of random "language-like" strings, like phonetic text or Markov dictionary strings, which are pronounceable but not actual words. Although, unlike completely random strings, characters like vowels will appear at higher frequencies when compared with other characters in pronounceable strings.

To impede automated attacks, many CAPTCHAs employ the use of visual clutter, e.g., in the form of background noise. From a usability perspective, humans must first be able to distinguish the text from any background clutter. Hence, too much clutter will make a scheme difficult to use. On the other hand, the use of color or background textures can make the task of perceiving the text from the background easier. However, it has been shown that the inappropriate use of color and background textures can be problematic in terms of both usability and security [17]. In general, if the color or background texture can easily be separated from the text using an automated program, it does not contribute to the security of the CAPTCHA. If so, it may be better not to use it, as it may harm usability by making it difficult to see the actual text or be distracting for humans.

3. Design variants

To overcome the limitations of traditional text-based CAPTCHAs, several different paradigms of CAPTCHAs have emerged. Some of these design variants are discussed in this section.

3.1. 3D-based

There have been a number of attempts at designing 3D-based CAPTCHAs. These approaches are typically implemented by rendering 3D models of text-objects, or of other objects, when generating the CAPTCHA challenges. The assumption of such CAPTCHAs is that the addition of the third dimension increases the difficulty for computers to identify 3D content, while being easy for humans as the perception of 3D is a natural part of the human visual system. Nevertheless, successful techniques for extracting textual content from 3D text-based CAPTCHAs to defeat them have previously been examined [12].

An example of a 3D CAPTCHA scheme, which is based on the rendering of 3D text-objects, was presented in Imsamai and Phimoltares [18]. However, it can be seen that in their approach that characters can easily be extracted, because no distortion was applied and the entire front face of characters were rendered using the same shade. Ross et al. [19] discuss previous approaches of using 3D models in CAPTCHAs and have pointed out problems due to the scalability of some approaches in terms of the amount of manual effort required to generate the challenges, and also observed that computer vision techniques can identify 3D objects in scenes. They proposed a prototype implementation called "Sketcha", which is based on oriented line drawings of 3D models. The user's task is to correctly orient images containing these 3D model line drawings. In other work, Susilo et al.

[20] examined an approach of generating 3D CAPTCHAs using stereoscopic images.

3.2. Animated

Animated CAPTCHAs are another design variant in which a time dimension is incorporated into the scheme. The main purpose of the time dimension is to distribute information required to solve a CAPTCHA challenge over multiple animation frames. Humans can easily process the information presented in the animated frames, whereas the assumption is that computers will have difficulty extracting this information. This has been dubbed the "zero knowledge per frame principle", because information required to solve an animated CAPTCHA is not completely contained within a single image [21]. However, it has been shown that information across multiple animation frames can be extracted to defeat such CAPTCHAs [11].

Examples of animated CAPTCHAs include a method based on moving letters amid a noisy background [21], the use of animation technology to provide better security over static images with distorted text [22], and an approach based on the idea of presenting distorted text on the face of a deforming surface [23]. Chow and Susilo [24] devised an animated 3D CAPTCHA named AniCAP, which was designed with the segmentation- resistant principle in mind. Their approach is based on motion parallax, the perception of depth through motion, where humans are supposed to distinguish the main characters located in the foreground from the background characters.

3.3. Other work

Other text-based CAPTCHA design variants include schemes where the challenge is to identify the location of characters, rather than to solely to identify the characters them- selves [25]. In addition, other than the traditional use of CAPTCHAs, it has been pro- posed that they can be used as graphical passwords [26].

Using machine learning, Bursztein et al. [27] presented a generic approach of using computers to solve text-based CAPTCHAs. They concluded that traditional purely text- based CAPTCHAs are likely to decline in utility, and that significant effort is required to rethink the way in which automated Turing tests are performed.

4. Conclusion

The research and design of CAPTCHAs have evolved over the years. Nowadays, CAPTCHAs remain a ubiquitous part of the Internet for deterring the automated abuse of online services intended for humans, and there are a variety of diverse schemes that have emerged over time. This article discusses text-based schemes in terms of their security and usability issues. In addition, this article also presents different design paradigms for text-based CAPTCHAs that have been proposed as alternatives to their traditional counterparts. With the debate surrounding the continual usage of CAPTCHAs and the various techniques for defeating CAPTCHAs that have been developed, the future of automated Turing tests is an open question.

References

[1] von Ahn L, Blum M, Hopper N J and Langford J 2003 CAPTCHA: Using hard AI problems for security *Lect. Notes Comp. Sc.* **2656** pp 294–311
[2] Naor M 1996 *Verification of a human in the loop or Identification via the Turing Test* http://www.wisdom.weizmann.ac.il/~naor/PAPERS/human.pdf
[3] Chew M and Baird H S 2003 BaffleText: A human interactive proof *SPIE Proc.* **5010** pp 305–316
[4] Chellapilla K and Simard P Y 2004 Using machine learning to break visual human interaction proofs (HIPs) *NIPS*

[5] Chellapilla K, Larson K, Simard P Y and Czerwinski M 2005 Building segmentation based human-friendly human interaction proofs (HIPs) *Lect. Notes Comp. Sc.* **3517** pp 1–26
[6] Yan J and Ahmad A S E 2007 Breaking visual CAPTCHAs with naive pattern recognition algorithms *ACSAC* pp 279–291
[7] Mori G and Malik J 2003 Recognizing objects in adversarial clutter: Breaking a visual CAPTCHA *CVPR* **1** pp 134–144
[8] Moy G, Jones N, Harkless C and Potter R 2004 Distortion estimation techniques in solving visual CAPTCHAs *CVPR* **2** pp 23–28
[9] Chellapilla K, Larson K, Simard P Y and Czerwinski M 2005 Computers beat humans at single character recognition in reading based human interaction proofs (HIPs) *CEAS*
[10] Bursztein E, Martin M and Mitchell J C 2005 Text-based CAPTCHA strengths and weaknesses *ACM Conf. on Computer and Communications Security* pp 125–138
[11] Nguyen V D, Chow Y-W and Susilo W 2012 Breaking an animated CAPTCHA scheme *Lect. Notes Comp. Sc. Applied Cryptography and Network Security - 10th Int. Conf. Proc.* **7341** pp 12–29
[12] Nguyen V D, Chow Y-W and Susilo W 2014 Security of text-based 3D CAPTCHAs *Computers & Security* **45** pp 84–99
[13] Chellapilla K, Larson K, Simard P Y and Czerwinski M 2005 Designing Human Friendly Human Inter-action Proofs (HIPs) *CHI ACM* pp 711–720
[14] Baecher P, Buscher N, Fischlin M and Milde B 2011 Breaking reCAPTCHA: A holistic approach via shape recognition *Future Challenges in Security and Privacy for Academia and Industry* **354** pp 56–67
[15] Cruz-Perez C, Starostenko O, Uceda-Ponga F, Aquino V A and Reyes-Cabrera L 2012 Breaking re-CAPTCHAs with unpredictable collapse: Heuristic character segmentation and recognition *Lect. Notes Comp. Sc.* **7329** pp 155–165
[16] Wang S-Y, Baird H S and Bentley J L 2006 CAPTCHA challenge tradeoffs: Familiarity of strings versus degradation of images *ICPR IEEE Computer Society* **3** pp164–167
[17] Yan J and Ahmad A S E 2008 Usability of CAPTCHAs or Usability Issues in CAPTCHA Design *SOUPS, ACM Int. Conf. Proceeding Series* pp 44–52
[18] Imsamai M and Phimoltares S 2010 3D CAPTCHA: A next generation of the CAPTCHA *Proc. of the Int. Conf. on Information Science and Applications (ICISA)* pp 1–8
[19] Ross S A, Halderman J A and Finkelstein A 2010 Sketcha: A CAPTCHA based on line drawings of 3D models *WWW ACM* pp 821–830
[20] Susilo W, Chow Y-W and Zhou H-Y 2010 STE3D-CAP: Stereoscopic 3D CAPTCHA *Lect. Notes Comp. Sc. Cryptology and Network Security* **6467** pp 221–240
[21] Cui J-S, Mei J-T, Zhang W-Z, Wang X and Zhang D 2010 A CAPTCHA implementation based on moving objects recognition problem *ICEE* pp 1277–80
[22] Athanasopoulos E and Antonatos S 2006 Enhanced CAPTCHAs: Using animation to tell humans and computers apart *Communications and Multimedia Security* **4237** pp 97–108
[23] Fischer I and Herfet T 2006 Visual CAPTCHAs for document authentication *8th IEEE Int. Workshop on Multimedia Signal Processing (MMSP 2006)* pp 471–474
[24] Chow Y-W and Susilo W 2011 AniCAP: An animated 3D CAPTCHA scheme based on motion parallax *Lect. Notes Comp. Sc. Cryptology and Network Security - 10th Int. Conf. Proc.* **7092** pp 255–271
[25] Nguyen V D, Chow Y-W and Susilo W 2014 A CAPTCHA scheme based on the identification of character locations *Lect. Notes Comp. Sc. Information Security Practice and Experience - 10th Int. Conf. Proc.* **8434** pp 60–74
[26] Zhu B B, Yan J, Bao G, Yang M and Xu N 2014 Captcha as graphical passwords - a new security primitive based on hard AI problems *IEEE T. Inf. Foren. Sec.* **9** pp 891–904
[27] Bursztein E, Aigrain J, Moscicki A and Mitchell J C 2014 The end is nigh: Generic solving of

text-based captchas *8th USENIX Workshop on Offensive Technologies*