CAPTCHA AND ITS APPLICATIONS

RAGAVI V¹ & G GEETHA²

¹Assistant Professor, Department of Computer Applications, Sathyabama University, Chennai, India
²Professor and Associate Dean, Department of Computer Science Engineering, School of Computer Science and Applications, Lovely Professional University, Phagwara, India

ABSTRACT

CAPTCHA is a challenge response system which is used to distinguish between human and automated programs. It is known for its efficiency in ensuring proper use of websites and online application by validating that the user is human and not a bot. Initially CAPTCHA was developed to mitigate Denial of Service, but now CAPTCHA is used for various applications. This paper brings out the various types and applications of CAPTCHA.

KEYWORDS: CAPTCHA, Applications of CAPTCHA, Challenge Test, Grade Test

INTRODUCTION

CAPTCHA stands for Completely Automated Public Turing Test to Tell Computers and Humans Apart [15]. Its underlying hardness is based on an Artificial intelligence problem. It is a program that can generate and grade tests that most humans can pass, but current computer programs can’t pass. They are commonly used to prevent the abuse of online services, such as a program creating thousands of free email accounts and then using them to send SPAM. For example, humans can read distorted text, but current computer programs can’t. Gimpy is the CAPTCHA based on the difficulty of reading distorted text. Bongo is based on visual pattern recognition problem. IMAGINATION is an image based CAPTCHA. Sound based CAPTCHA was introduced by Nancy Chan of the City University, Hong Kong. Each type of CAPTCHA has its own application.

TYPES OF CAPTCHA

CAPTCHA is mainly categorized into four types, namely Text Based, Image Based, Audio Based and Video Based.

Text Based CAPTCHAs: They require users to read and type distorted text rendered in an image. It is the most widely deployed. Major web sites such as Google, Yahoo and Microsoft all have their own text-based CAPTCHAs deployed for years [3, 4, 7]. Some of the text based CAPTCHAs popularly used are shown in the Figure 1.

![Figure 1: Text Based CAPTCHAs](image-url)
**Image Based CAPTCHAs:** The users are asked to perform an image recognition task. Image based CAPTCHAs have been proposed as alternatives to the text media [9, 19]. In Figure 2 Some of the Image based CAPTCHAs are shown.

![Image Based CAPTCHA Examples](image1.png)

**Audio Based CAPTCHAs:** They rely on sound or speech recognition by the users. Audio CAPTCHAs were introduced as an accessible alternative for those who are unable to use the more common visual CAPTCHAs and for the visually impaired. Figure 3 Shows some of the audio enabled CAPTCHAs

![Audio Based CAPTCHA Examples](image2.png)

**Video Based CAPTCHAs:** The user is given a moving object and is asked to perform a task. Video based CAPTCHA was developed mainly to make CAPTCHA session interesting and innovative [14]. Figure 3 Shows some of the video CAPTCHAs.

![Video Based CAPTCHA Examples](image3.png)

**APPLICATIONS OF CAPTCHA**

CAPTCHAs have several applications [18] for practical security, some of them are listed below:-

**Mitigating Comment Spam**

Comment Spam is irrelevant comments posted to a blog for the sole purpose of dropping a link to the spammer’s
website. Most bloggers are familiar with programs that submit bogus comments, usually for the purpose of raising search engine ranks of some website. Comment spam is also called a spamment, a combination of the words ‘spam’ and ‘comment’. CAPTCHA is used to prevent comment spam [11]. By using one the above mentioned CAPTCHA, only legitimate users (i.e. Human) can enter comments on a blog or forum. Automated programs cannot solve the CAPTCHA so they are kept at bay.

Online Polling

CAPTCHA is used in online polling to make sure that the voted person is a human or not. This helps in preventing biased results by automated programs and ensures that only humans took part in the polling. This is discussed by the authors in[2, 6].

Web Registration

Many companies offer free registration services. Most of these services suffer from a type of attack called flooding attack, where the bot would sign up thousands of registration forms every second. This results in denial of service. In February 2000, a string of distributed denial of service attacks crippled popular websites including CNN.com, Amazon.com, eBay.com, and yahoo.com for several hours. Another large distributed denial of service attack in October 2002 took out nine of the thirteen root DNS servers. The solution to this problem is to use CAPTCHA. CAPTCHA ensures that only humans sign up the registration forms and not automated programs (bots). This is well said in [5, 12, 13]

Boxbe

Boxbe is a way to protect email addresses from spam scrapers. It provides a whitelist based email filter. It presents challenges (CAPTCHA) to sender that requires a human response. Users of the service can share their whitelist with other Boxbe users, using their friend of a friend network to screen their email. Boxbe works as follows. If the receivers email box is boxbe protected, then if you have added your friends and family to your Guest List, the email will reach you as it would without Boxbe's service. The people you have not pre-approved receive an invitation to join your Guest List. The invitation lets the sender take a simple test (CAPTCHA Challenge) to confirm they are not a spambot. Once a sender receives an invitation and solves the CAPTCHA challenge, the email is delivered.

Preventing Dictionary Attacks

A dictionary attack is a method by which password protected computers or servers are hacked by systematically entering every word from a dictionary as password. Normally many people have the practice of using ordinary words as password. CAPTCHA can be used to prevent dictionary attacks. After a certain number of unsuccessful logins, the system may ask the user to solve a CAPTCHA. If the user is human, he may solve the challenge. If it was a bot it may be caught. Normally for dictionary attacks only bots are employed, as every word in the dictionary has to be tried. This is discussed in [6, 22]

Protecting Confidential Web Pages

In a website certain pages are confidential, which are kept unindexed to prevent others from finding them easily. There are HTML tags that are used for preventing bots entering into the confidential pages, but it cannot guarantee it. CAPTCHA are used here. If the user is a person who really needs the information, he will solve the CAPTCHA challenge and gain access to the page. If the search engine is a bot, then it will not gain access.
Preventing Phishing

The art of masquerading as a trust worthy third party in order to acquire users personal information such as usernames, passwords, credit card details and many more, is called Phishing. Phishing is one of the attacks that became popular recently. It has become a serious threat to enterprises that deal with financial transactions. CAPTCHA can be used to prevent phishing attack. This is discussed by Chun-Ming Leung in [8]

Filtering SMS Spam

Short Message spam is another threat posed in the current scenario. CAPTCHA is used to filter short message spam of group sending. If the Short Message Service (SMS) can pass the CAPTCHA, it will be identified as legitimate SMS and transmitted by Short Message processing Center. Conversely, if the SMS cannot pass the CAPTCHA, it will be identified as SMS spam and deleted by Short Message processing Center [17, 20, 21].

Smart Cards

Smart cards are small plastic cards with embedded integrated circuits, which are used for making financial transactions. Smart cards are the credit cards and debit card which everyone uses in their day today life. CAPTCHA is used while making financial transactions with smart cards, to provide additional security other than username and password. This way CAPTCHA is used to defend ecommerce effectively. Vo has discussed about Smart Card fraud and how to use CAPTCHA to prevent it in [23].

Prevent Spam in VoIP

Voice over Internet Protocol (VoIP) is one of the budding technologies today. This application offers the user a service by which one can call another person at a low cost as compare with traditional phone services. One of the drawbacks in this technology is the unsolicited and unwanted calls by the users. This is referred to as spam in VoIP. CAPTCHA is used here to determine whether the call is coming from a human or from a bot [1].

Preventing Sybil Attack

Sybil attack is an attack when one node in a network claims multiple identities. Peer-to-peer network is the most popular file sharing medium in the Internet. This medium suffers when one node in the network forges with multiple identities. CAPTCHA is used here to identify the malicious entities in the network. This concept is discussed by Haribabu et al in [10].

Preventing Bots in Social Network

Botnet, a network of compromised computers, is identified as a major threat in Internet today. These botnet communicate with its owner via communication channel called Command and Control channel. There are three types of such C&C channel, Internet Relay Chat (IRC), Peer-to-Peer (P2P) and web based protocols. By using the loop hole in the web2.0 technology, these botnet conquer the social networks. In August 2009, Twitter the famous social network was conquered by botnet. CAPTCHA is used to mitigate such attacks; the method of mitigation is discussed by Vo. N. H and Pieprzyk. Jin [23]

Online Games

Bots used in online games is a massive threat today. Honest players are being cheated. Bots when employed in playing games do not get tired and thus conquer huge amount of game wealth, resource and points, without much effort.
On the other hand man gets tired very fast and thus has to give to the bots. This is illegal. CAPTCHAs are used in online games to verify the opponent is a man or a machine, so as to play a fair game. This is discussed in [25].

CONCLUSIONS

CAPTCHA tests are based on artificial intelligence (AI): decoding images of distorted text, for instance, is well beyond the capabilities of modern computers. CAPTCHA though has many applications in varied fields; it is primarily used to distinguish between man and bot. CAPTCHAs also offer well-defined challenges for the AI community, and invites security researchers as well as malicious programmers, to work on advancing the field of Artificial Intelligence.

REFERENCES


