Threat Modeling for Breaking of CAPTCHA System

Divya Suvarna(✉) and Sujata Pathak(✉)

Department of Information Technology,
K. J. Somaiya College of Engineering, Mumbai, India
{divya.suvarna, sujatapathak}@somaiya.edu

Abstract. The online websites are accessed by millions of people and the information present on it holds value. To secure them from attacker, one such mechanism is "Completely Automated Public Turing Test to keep the Computers and Humans Apart". They are used to ensure that internet user's activity is performed by humans only and not the bots. CAPTCHAs are solved by people every day to prevent Denial of Service attack and online spam attack. But unfortunately, it is now possible to break them by using Machine Learning. This paper presents, the Vulnerabilities related to Text-based CAPTCHA System, compromised system using Machine Learning and proposed Algorithm. A Threat Modeling was performed on the website using a Text-based CAPTCHA System in order to discover various Attack Vectors with the help of a Tool and performs detailed analysis on affected areas. Lastly, a solution is provided to the website service provider to overcome the exsisting system flaws and also to make them even more strong and secure.

Keywords: CAPTCHA · Machine Learning Algorithm · Cyber Attacks · Threat Modeling · Word Cloud

1 Introduction

Many websites, online services, e-banking services, online tolling and digitize books use the completely Automated Public Turing tests to identify whether the user is Computer or Human. For Example, Facebook restrict the creation of fake profiles to spam legitimate users, Google use re-CAPTCHA to improve its services by blocking access to automated spammers, and Yahoo mail improves by blocking bots from spamming the Mail.

Today we have a different form of CAPTCHAs such as Image, Audio, Video, 3D, Text based CAPTCHA. And threats against the text based CAPTCHA is increasing. As it is understood annoying but yet bulletproof. But this understanding is challenged today. Various research studies state that there is no standard methodology for designing and evaluating it. With the use of existing technology hackers can easily break the existing security mechanism. By finding the vulnerability in the existing system it is possible to disrupt the availability of the services. Prakash et al. in this paper, authors have studied different types of CAPTCHA and a survey has been done

A. P. Pandian et al. (Eds.): ICICCS 2019, AISC 1039, pp. 94–104, 2020.
https://doi.org/10.1007/978-3-030-30465-2_12