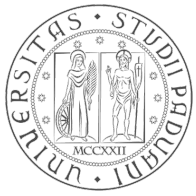


University of Padova

Engineering Departement

Computer Engineering Master Degree

Invisible CAPPCHA

Candidate

Di Nardo Di Maio Raffaele

Supervisor

Prof. Migliardi Mauro

Co-Supervisors

Guerar Meriem

DD-MM-YYYY

Accademic Year 2020-2021

To my parents, that always help
me to be happy doing what I love
and support me reaching my goals.

“*Most people assume that once security software is installed, they're protected. This isn't the case. It's critical that companies be proactive in thinking about security on a long-term basis.*”
Kevin Mitnick

“*You have to learn the rules of the game. And then you have to play better than anyone else.*”
Albert Einstein

“*Si come il ferro s'arrugginisce sanza esercizio, e l'acqua si putrefà o nel freddo s'addiaccia, così lo 'ngegno sanza esercizio si guasta.*”
Leonardo da Vinci

Contents

Chapter 1

Introduction

CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) is a program used to distinguish human users from bots. A bot is a malicious application that automates a task, gathering useful information about user credentials or pretending to be a human interaction with Web application. Hence the term *"bot"* is an abbreviation of the words "software robot".
The CAPTCHAs are traditionally used in Web applications for[5]:

- **Online Polls**
  CAPTCHAs prevent the creation and the submission of a large number of votes, favouring a party.
- **Protecting Web Registration**
  CAPTCHAs prevent the creation of free mail account to bot instead of human users. The goal of the use of CAPTCHAs is to remove the possibility that the hacker could take advantages from the large amount of registrations.
- **Preventing comment spam**
  CAPTCHAs prevent the insertion of a large amount of posts made by bot on pages of social platforms or blogs.
- **Search engine bots**
  CAPTCHAs are used to guarantee that a website should be unindexed to prevent the reading of the page through search engine bots. The CAPTCHAs are added because the html tag, used to unindex the web page, doesn't guarantee unindexing.
- **E-Ticketing**
  CAPTCHAs prevent that a big events would sell out minutes after

tickets become available. In fact ticket scalpers that make large number of ticket purchases for big events.

- **Email spam**
  CAPTCHAs are used to verify that a human has sent the email.

- **Preventing Dictionary Attacks**
  CAPTCHAs prevent bot to guess the password of a specific user. The hacker could guess the password, taking it from a dictionary of passwords. The use of the CAPTCHA challenge prevents the iteration of the login phase made by the bot using all the words of the dictionary. After a certain number of failures POST requests, the CAPTCHA challenge is shown to the user.

- **Verifying digitized books**
  ReCAPTCHA can verify the contents of a scanned piece of paper analysing responses in CAPTCHA fields. A computer cannot identify all the words from a digital scan.
  The application submits two words to the user in the CAPTCHA challenge: the first one that the machine has already recognized and the other for which it can correctly associate a word. If the user types the two words and the first one was correctly detected, it assumes that also the second one is correct.
  In this case the second word is added to a set of words that are going to be added to other users' challenges. If the application receives enough responses with the same typed word related to the unknown word, the program extablishes that typed word is the CAPTCHA is related only to the first word and the challenge related to the second word is exploited by the application to scan digitally the paper.

Another useful application of CAPTCHA is the support to the authentication process. This application is going to be analysed in details in the next chapters, looking at the authentication from smartphone.
In Chapter 2 there is a description of the state of art of CAPTCHA, looking at types of CAPTCHA and the related tests from which this challenge is born.
In Chapter 3 Invisible CAPPCHA is described in details.
DESCRIPTION OF THE CONTENT OF THE CHAPTERS

Chapter 2

State of Art

CAPTCHA takes inspiration and is related to three main elements[6]:

1. **Turing test**
   it's used to determine how much a machine can think like a human. The test is made by three figures: a human examiner, an human and a machine. The examiner asks some questions to both other two figures and, after a fixed amount of time, evaluates if the two answers are different or not.
   If they are similar w.r.t. the point of view of the examiner, the machine is an AI (Artificial Intelligence) similar to an human. The test is very important if the answers have many possibilities.

2. **Human-Computer Interaction (HCI)**
   according to cognitive psychology studies, a human process data in a specific way and this test evaluates the interaction between humans and machines. The HCI model is divided into five levels:

   - task level
   - semantic level
   - syntactic level
   - interactive level
   - a level of physical devices

   Then the obtained information is processed by:

   - reasoning
   - problem solving
   - skill acquisition

- error

3. **Human Interactive Proof (HIP)**
   it's used to make differentiation between machine and human users and computer user programs. The test require a type of interaction, that is simple to be done by human instead of bot. The main goals of this type of test are:

   - To differentiate the humans from the computers
   - To differentiate a category of the humans
   - To differentiate a specific human from the category of humans

   HIP has the test program that is subjected to the human and the computer. As a result, only a specific group of humans can positively solve the test and then the test results can be validated by the computer.

In order to guarantee a good level of security, a CAPTCHA has to satisfy the following requirements:

- The solution to the CAPTCHA isn't conditional and shouldn't depend on the user's language and/or age.
- The solution of the CAPTCHA must be easy for the humans and hard for the bots. Hence, humans in no longer than 30 seconds with very high success rate
- The creation of the CAPTCHA must not disturb the user privacy (not linked to the user).

2.1 Traditional CAPTCHAs

The traditional CAPTCHAs are based on the knowledge and correct insertion of solution by the user. Some types of CAPTCHA have a big issue because they don't destroy the session, after the correct answer is inserted by the user[5]. Hence, the hacker can crack following accesses using the same session id with the related solution of the challenge, after connecting to the web page of CAPTCHA. In this way the attacker can make hundreds of requests before the session expires and the previous operation must be computed again.
The main types of these CAPTCHAs are described in the following sections but the details about specific implementations can be found in the article of Walid Khalifa Abdullah Hasan[8]. With respect to user experience, the most

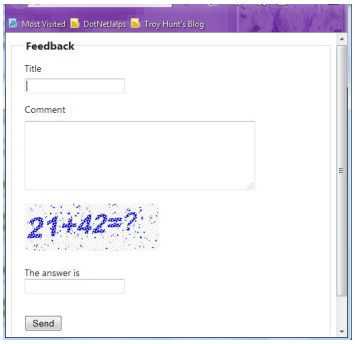
enjoyable traditional CAPTCHAs are usually the game-based and image-based ones but the most frustrating CAPTCHA is the text-based one[13]. A summary of usability and security issues is shown in Table 2.1.

2.1.1 Arithmetic (Math)

Looking to an operation specified in a frame, the user needs to insert the result in a text field. The operation is written in plain text or, to improve the security of this challenge, it's warped like text-based CAPTCHAs (Figure 2.1). These classical math-CAPTCHAs, also known as *arithmetic CAPTCHAs*, are vulnerable to OCR (Optical Character Recognition) techniques.

An advanced version of this CAPTCHA is used in the Quantum Ran-

(a) With plain text.



(b) With wrapped text.

Figure 2.1: Example of arithmetic CAPTCHAs.

dom Bit Generator Service (QRBGS) sign-up Web Page[11] (see Figure 2.2). This type of CAPTCHA asks user to solve an advanced math expression. It prevents the use of free or commercial OCRs because many mathematical symbols are not considered in their detection algorithm.
Hence many math symbols are wrongly translated by bot programs and the challenge is very secure. The only problem is that this CAPTCHA is very complex for normal users and many of them could not solve the challenge correctly.

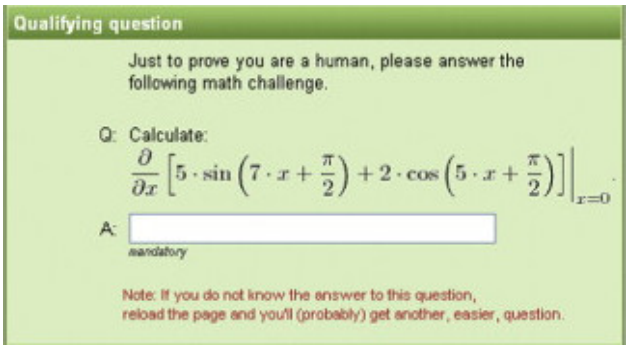


Figure 2.2: Example of Quantum Random Bit Generator Service (QRBGS) sign-up Web Page [11].

2.1.2 Audio-based

This type of CAPTCHAs asks the user to type the words listened by an audio file (see Figure 2.3). It's developed for vision-impaired users. It usually has problems related to the language dictionary, from which words are taken, and the similarity of the sound between several words. This type of CAPTCHAs is vulnerable to many Automatic Speech Recognition (ASR) programs[3] but also Deep Learning techniques (e.g. DeepCRACk[4]).

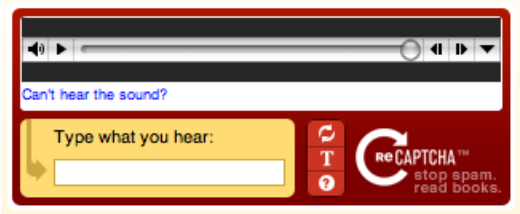


Figure 2.3: Example of audio-based CAPTCHA.

2.1.3 Game-based

This type of CAPTCHAs performs the verification of the user nature through a set of several kind of games (see Figure 2.4). This type of CAPTCHAs is called *Dynamic Cognitive Game (DCG)* is usually developed using Flash and HTML5 with JavaScript. These technologies download the game code to the client and execute it locally. The only difficult for the bot to attack the challenge is the encryption/obfuscation of the code. This strategy prevent the store of the code onto different internet domains. However for example, there exists a bot attack, called *Stream Relay Attack*, that obtains good results bypassing these challenges [12].

Figure 2.4: Examples of game-based CAPTCHAs.

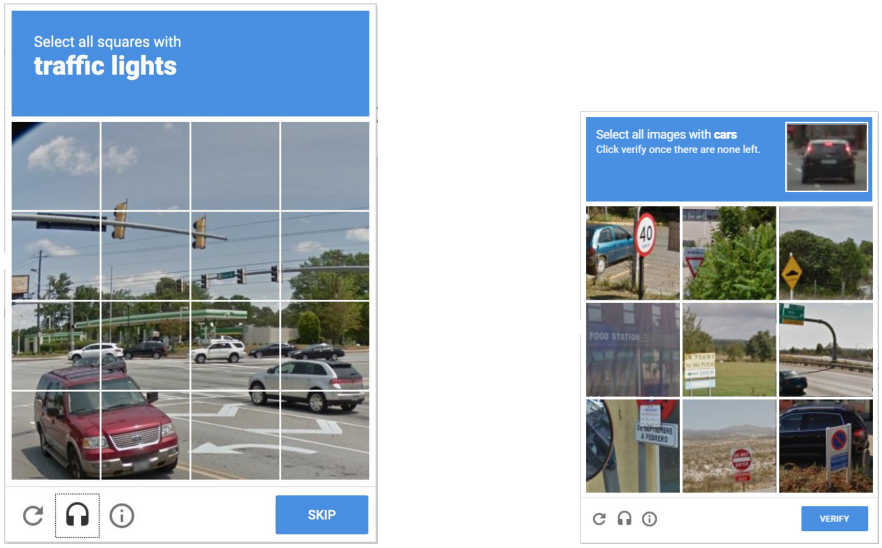
2.1.4 Image-based

This type of CAPTCHAs asks to select the images that contain a requested subject. The set of images, on which the user needs to identify the subject, can be implemented in different ways, for example:

- An image is divided into a set of sub-squares and each of them is a candidate image2.5a
- There are many images, each one with a unique different subject (see Figure 2.5b)

This type of CAPTCHAs is vulnerable to different Object Recognition techniques developed for Computer Vision purposes. An extension of this type of CAPTCHAs, called *FaceDCAPTCHA*, has been introduced[9]. It incorporates elements of face detection. The human brain is very effective in the process of natural face segmentation even if there are complex backgrounds. This approach increases the security efficiency because the Computer Vision programs can easily detect if there is a face, e.g. Viola-Jones algorithm[10], but have many problems differentiating real and non-real photographs of faces.
Face, fingerprint and eye detections in images remain also a difficult challenge

to be performed by computers. For this reason these results were used to develop a new variant of image-based CAPTCHA called *MB CAPTCHA*[17].



(a) With an image divided in sub-squares. (b) With several images.

Figure 2.5: Examples of image-based CAPTCHAs.

2.1.5 Puzzle-based

This type of CAPTCHAs asks the user to complete a visual puzzle, created by dividing a given image in a set of pieces[7] (see Figure 2.6a).
The task isn't easy for users because this type of CAPTCHAs takes more time to solve the puzzle but the security level is very high[7]. To improve the usability of the CAPTCHA, there exists a variant of the puzzle-based CAPTCHA in which needs to insert only some pieces of the puzzle instead of completing the whole puzzle (see Figure 2.6b).

2.1.6 Text-based

This type of CAPTCHAs shows a series of wrapped characters and/or numbers on the screen (see Figure 2.7). The users needs to understand which are the characters that composes the shown sequence and then type them inside a text-field. This type of CAPTCHAs is vulnerable to several type of attacks, related to Computer Vision techniques, that are:

- OCR techniques[2]

(a) Completing the puzzle. (b) Inserting only some pieces.

Figure 2.6: Examples of puzzle-based CAPTCHAs.

- Segmentation techniques (e.g. DECAPTCHA[1])
- Machine Learning and Deep Learning techniques

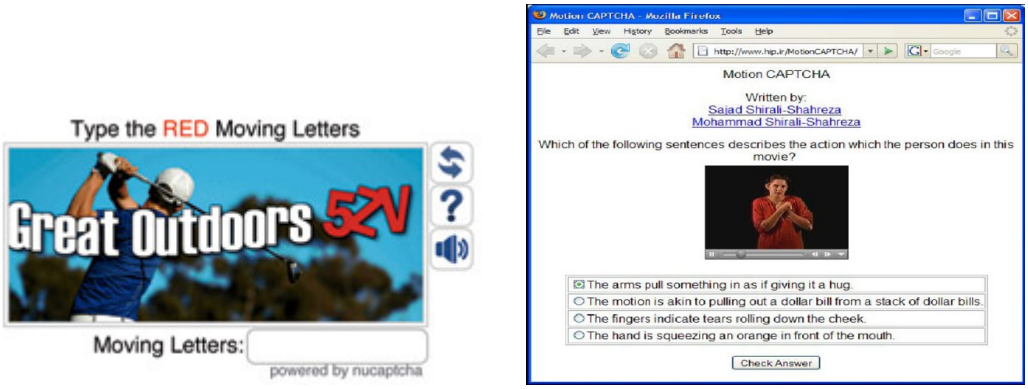
In the design phase of a text-based CAPTCHA there are many issues, related to Computer Vision techniques, to be considered. For each of them, there is usually a solution in the design phase of the CAPTCHA that reduces the possibility that the challenge would be broken by a bot[1].

Figure 2.7: Example of text-based CAPTCHA.

2.1.7 Video-based

This type of CAPTCHA is not very common because of the weight of the file to be downloaded[8]. The traditional video-based CAPTCHA is composed by a video in which a sliding text is shown (see Figure 2.8a). The user needs to type this message in a text field to pass the challenge. Some implementations of this type of CAPTCHAs are vulnerable to machine learning attacks.

Another similar and interesting variant of this CAPTCHA is the *Motion CAPTCHA*[14], developed by M. Shirali-shahreza and S. Shirali-shahreza, in which the user needs to watch a video. Then he needs to select which action was performed in the played file, choosing it from multiple answers (see Figure 2.8b). The strength of these implementations of CAPTCHAs depends on the relationship between the multiple choices submitted to the user[15].



(a) Example of sliding text in video. (b) Example of Motion CAPTCHA[14].

Figure 2.8: Examples of video-based CAPTCHAs.

2.2 Modern CAPTCHAs

The type of CAPTCHAs and authentication mechanisms described in the following section are far from traditional CAPTCHAs and aren't based on cognitive knowledge of the human user but on other parameters. In the following sections there is an overview of the most mechanisms of this type.

2.2.1 Biometrics-based

This type of authentication mechanisms are based on biometric parameters of the user. In literature the most known implementations are:

- **Bio-CAPTCHA voice-based Authentication**
  This authentication method was developed starting from good results reached in the authentication phase of cloud systems (Alexa for Amazon, Siri for Apple, Cortana for windows)[16]. This particular implementation uses a random voice-based password challenge. This password changes at every login of the user and this method uses

CAPTCHA challenge to provide unpredictability and ambiguity to the authentication process. The experiments reveals that unauthorized access probability decreases, while it keeps high usability because it needs only a mic.

- **rtCAPTCHA**
  this type of authentication method is a Real-time CAPTCHA that asks users to perform some tasks like smile, blink or nod in front of the camera of the mobile phone. The recorded video is sent to the service provider that checks if in the file, there is the expected user performing the required action.
  This implementation of CAPTCHA solves many problems of similar CAPTCHAs that are also based on liveness mechanisms and video capture. The attackers can extract patterns or features from existing or captured images and embed them into a new generated video in attack in the compromised device.
  In the work of Erkam Uzun, Simon Pak Ho Chung, Irfan Essa and Wenke Lee[18], there is a detailed comparison between other similar authentication mechanisms and rtCAPTCHA, looking to all possible Computer Vision attacks.

2.2.2 Behavioural-based

- **Google no CAPTCHA**
  Google developed in 2015 a new CAPTCHA system that is simpler than traditional CAPTCHAs in terms of user interaction[19]. This CAPTCHA system is composed by two layers of protection:

  1. Checkbox to be clicked by user as in Figure 2.9 (or image-based CAPTCHA on mobile devices)

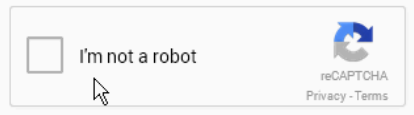


Figure 2.9: Example of Google no CAPTCHA checkbox.

  2. Traditional text-based CAPTCHA with two warped words

The second layer is reached only if the user doesn't succeed in the first one. For the checkbox step, the application evaluates the time needed by user to successfully click the checkbox and also the position of the

cursor. The application performs an *advanced risk analysis*, by looking results of first step but also spam traffic and passed/failed CAPTCHAs. It understands in this way if the test is passed or not.
The tests done confirms that this phase was very inefficient and many times the first layer failed even if a human user was performing correctly the task. A problem of this type of CAPTCHA is that many attacks exploits the image-based CAPTCHA and text-based CAPTCHA using attacks based on known Computer Vision techniques or their variants (e.g. CAPTCHA breaker made by Suphannee Sivakorn, Jason Polakis and Angelos D. Keromytis[**?**]).

- **Google Invisible ReCAPTCHA**
  It's a top layer over the *Google noCAPTCHA v2.0*, adding the option to bind directly to the form's submit element[19]. There exist two version of this CAPTCHA:

  - **ReCAPTCHA v2.0**
    it was developed in 2017. It's not really invisible because Privacy & Policy badge must be included on every page of app or website in which the CAPTCHA is used. Computer Vision and Artificial Intelligence algorithms can break the challenges by recognizing object in the pictures in the image-based CAPTCHA phase.
  - **ReCAPTCHA v3.0**
    it was developed in 2018. With constantly analyzing human behavior, mouse movements, typing speed and other features incorporated into NO CAPTCHA technology, Google collected enough sample data to perfectly fine-tune their Google invisible reCAPTCHA v2.0 with this new version. This type of CAPTCHA uses Artificial Intelligence and Machine Learning probability scores, hostname, timestamp and anction validations.
    Google removes image recognition and looking only the score, it evaluates if the user is a human or a bot. The main difference w.r.t. previous versions is that this CAPTCHA returns a probability score (*risk score*) in the range $[0.0, 1.0]$: *0.0* if the user is a bot, *1.0* otherwise. The administrator of the website can decide what range of scores he wants to manage, declaring the the site is under attack and what actions need to be performed.
    Some characteristics related to this version of *Invisible ReCAPTCHA* are:

    * If a user accesses a Web page using incognito mode or private mode, he is classified with a very low score (*high risk*).

    * If a human is wrongly classified as a bot, the user can login into its Google account to increase its score. If this doesn't change the classification, you cannot do anything else.

- **Completely Automated Public Physical test to tell Computer and Humans Apart (CAPPCHA)**
  this is a way to enforce the PIN authentication phase by mobile phone[21]. The user needs to tilt the device to a specified angle specified on the screen. The CAPPCHA security is based on the *Secure Element* (*SE*) present in the device. It prevents brute force, side channel and recording attacks. The usability results are good and then some of the comments made by users were considered in the implementation.

- **Invisible CAPPCHA**
  it's an evolution of the CAPPCHA, in terms of usability, and the CAPTCHA challenge is hidden behind the PIN authentication phase[22]. The micro-movements of the device, generated by the interaction of the user with the touch-screen, are evaluated and the *Secure Element* (*SE*) tells to Service Provider if the input is inserted by a human or not. More details about Invisible CAPPCHA are reported in Chapter 3.

CAPTCHA type	Usability issues	Security
Arithmetic (Math)	To be more effective, it requires advanced math knowledge.	Vulnerable to OCR techniques.
Audio-based	Issues of recognition: • Previous knowledge of English dictionary by the user. • Some character sounds very similar to others.	It's vulnerable to: • ASR programs. • Deep learning techniques.
Game-based	No problem	Vulnerable to Stream Relay Attack
Image-based	Difficulty of identification of images caused by: • Blur of images. • Low vision condition.	
Puzzle-based	Too much time to solve the puzzle	No significant issues
Text-based	Many problems have to be solved by user: • Multiple fonts. • Font size. • Blurred Letters • Wave Motion.	It can be identified by: • OCR technique • Segmentation techniques • Machine Learning and Deep Learning techniques
Video-based	Heavy file to be downloaded	

Table 2.1: Survey of main types of traditional CAPTCHAs[7].

Alternative Type	Name of implementation	Usability issues	Security

Table 2.2: Survey of main types of alternatives of CAPTCHAs[7].

Chapter 3

Invisible CAPPCHA

Bibliography

[1] E. Bursztein, M. Martin, J. Mitchell,"Text-based CAPTCHA strengths and weaknesses" in *Proc. 18th ACM Conference on Computer and Communications Security (CCS), 2011, pp. 125–138.*

[2] Silky Azad, Kiran Jain„"Captcha: Attacks and weaknesses against OCR technology" in *Global Journal of Computer Science and Technology, 2013.*

[3] Jennifer Tam, Jiri Simsa, David Huggins-Daines, Luis von Ahn, Manuel Blum,"Improving Audio CAPTCHAs" in *Symposium On Usable Privacy and Security (SOUPS), 2008.*

[4] William Aiken, Hyoungshick Kim,"POSTER: DeepCRACk: Using Deep Learning to Automatically CRack Audio CAPTCHAs" in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security (ASIACCS), 2018.*

[5] Sarika Choudhary, Ritika Saroha, Yatan Dahiya, and Sachin Choudhary, "Understanding CAPTCHA: Text and Audio Based Captcha with its Applications" in *International Journal of Advanced Research in Computer Science and Software Engineering, 2013, vol. 3(6), pp. 106-115.*

[6] Darko Brodić, Alessia Amelio, Radmila Janković, "Exploring the influence of CAPTCHA types to the users response time by statistical analysis" in *Multimedia Tools and Applications, vol. 77, pp. 12293–12329, 2017.*

[7] Ved Prakash Singh, Preet Pal, "Survey of Different Types of CAPTCHA" in *International Journal of Computer Science and Information Technologies (IJCSIT), vol. 5(2), 2014.*

[8] Walid Khalifa Abdullah Hasan, "A Survey of Current Research on Captcha" in *International Journal of Computer Science Education in Schools (IJCSES), vol. 7, pp. 141–157, 2016.*

[9] Goswami G, Powell BM, Vatsa M, Singh R, Noore A, "FaceDCAPTCHA: face detection based color image CAPTCHA" in *Future Generation Computer Systems, vol. 31(2), pp. 59–69, 2014.*

[10] Wen-yao Lu, Ming Yang, "Face Detection Based on Viola-Jones Algorithm Applying Composite Features" in *International Conference on Robots & Intelligent System (ICRIS), pp. 82-85, 2019.*

[11] Carlos Javier Hernandez-Castro, Arturo Ribagorda, "Pitfalls in CAPTCHA design and implementation: The Math CAPTCHA, a case study" in *Computers & Security, vol. 29(1), pp. 141-157, 2010.*

[12] Manar Mohamed, Song Gao, Nitesh Saxena, Chengcui Zhang, "Dynamic cognitive game captcha usability and detection of streaming-based farming" in *The Workshop on Usable Security (USEC), co-located with NDSS, 2014.*

[13] Ruti Gafni, Idan Nagar, "CAPTCHA – Security affecting user experience" in *Issues in Informing Science and Information Technology, vol. 13, pp. 63-77, 2016.*

[14] M. Shirali-Shahreza and S. Shirali-Shahreza, "Motion CAPTCHA" in *2008 Conference on Human System Interactions, Krakow, pp. 1042-1044, 2008.*

[15] Kameswara Rao Kavya Sri, Gnana Sai, "A Novel Video CAPTCHA Technique to Prevent BOT Attacks" *International Conference on Computational Modeling and Security (CMS 2016), Procedia Computer Science, vol. 85, pp. 236–240, 2016.*

[16] Omar Ahmed Hedaia, Ahmed Shawish, Hana Houssein, Hala Zayed, "Bio-CAPTCHA Voice-Based Authentication Technique for Better Security and Usability in Cloud Computing" in *International Journal of Service Science Management Engineering and Technology, vol. 11(2), pp. 59-79, 2020.*

[17] Brian M. Powell, Abhishek Kumar, Jatin Thapar, Gaurav Goswami, Mayank Vatsa, Richa Singh, Afzel Noore, "A multibiometrics-based CAPTCHA for improved online security" in *IEEE 8th International Conference on Biometrics Theory, Applications and Systems, 2016.*

[18] Erkam Uzun, Simon Chung, "rtCaptcha: A Real-Time Captcha Based Liveness Detection System" in *The Network and Distributed System Security Symposium (NDSS), Georgia Institute of Technology, 2018.*

[19] https://tehnoblog.org/google-no-captcha-invisible-recaptcha-first-experience-results-review/

[20] Suphannee Sivakorn, Jason Polakis, Angelos D. Keromytis, "I'm not a human: Breaking the Google reCAPTCHA" in *Black Hat, pp. 1–12, 2016.*

[21] Meriem Guerar, Alessio Merlo, Mauro Migliardi, "Completely automated public physical test to tell computers and humans apart: A usability study on mobile devices" in *Future Generation Computer Systems, vol. 82, pp. 617–630, 2018.*

[22] Meriem Guerar, Alessio Merlo, Mauro Migliardi, Francesco Palmieri, "Invisible CAPPCHA: A usable mechanism to distinguish between malware and humans on the mobile IoT" in *Computers & Security, vol. 78, pp. 255–266, 2018.*

Acknowledgements

Professor Migliardi

I would like to express my very great appreciation to Dr Guerar

I would like to express my gratitude to University of Padova for the study path I performed. The uncertainty about the future and the idea of being far from needed cyber security skills have become a stimulus to improve myself. I learn a lot and I got hooked on the programming, starting from zero level of it, thanks to the professors' professionalism and knowledge. During the last five years, I've changed and now I spend programming all my free time. Thanks to University because professors follow my thirst of knowledge and I grew up, living alone and really becoming an adult.

Thanks to staff,

Thanks to other company,

Thanks to my family

Thanks to my grandmother

Thanks to Cristina,

Thanks to Francesca,

Thanks to Davide,

Thanks to Giuseppe, Aurora, Alessia and Sara,

Thanks to Elia,

Thanks to Lorenzo,