Gotta CAPTCHA 'Em All: A Survey of Twenty years of the Human-or-Computer Dilemma

Journal:	*IEEE Communications Surveys and Tutorials*
Manuscript ID	COMST-00559-2020
Type of Manuscript:	Survey
Date Submitted by the Author:	12-Oct-2020

Complete List of Authors:	Guerar, Meriem; University of Genoa, Department of Informatics, Bioengineering, Robotics and Systems Engineering Verderame, Luca; University of Genoa, Department of Informatics, Bioengineering, Robotics and Systems Engineering Migliardi, Mauro; University of Padua, Department of Electronic Engineering Palmieri, Francesco; university of salerno, computer science Merlo, Alessio; University of Genoa, Department of Informatics, Bioengineering, Robotics and Systems Engineering

Keywords:	CAPTCHA, Security, Bot

Gotta CAPTCHA 'Em All: A Survey of Twenty years of the Human-or-Computer Dilemma

Meriem Guerar, Luca Verderame, Mauro Migliardi, Francesco Palmieri, and Alessio Merlo

***Abstract*—**
A Recent study has found that malicious bots generated nearly a quarter of overall website traffic in 2019 [1]. These malicious bots perform activities such as price and content scraping, account creation and takeover, credit card fraud, denial of service, etc. Thus, they represent a serious threat to all businesses in general, but are especially troublesome for e-commerce, travel and financial services. One of the most common defense mechanisms against bots abusing online services is the introduction of Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA), so it is extremely important to understand which CAPTCHA schemes have been designed and their actual effectiveness against the ever-evolving bots. To this end, this work provides an overview of the current state-of-the-art in the field of CAPTCHA schemes and defines a new classification that includes all the emerging schemes. In addition, for each identified CAPTCHA category, the most successful attack methods are summarized by also describing how CAPTCHA schemes evolved to resist bot attacks, and discussing the limitations of different CAPTCHA schemes from the security, usability and compatibility point of view. Finally, an assessment of the open issues, challenges, and opportunities for further study is provided, paving the road toward the design of the next-generation secure and user-friendly CAPTCHA schemes.

***Index Terms*—CAPTCHA, Bot, CAPTCHA Type, Security, Text CAPTCHA, Image CAPTCHA, Behavior CAPTCHA, Sensor CAPTCHA.**

I. Introduction

A *Completely Automated Public Turing tests to tell Computers and Humans Apart* (CAPTCHA) is, as the name suggests, a challenge-response test used to distinguish between genuine human users and automated computer programs. CAPTCHAs are commonly used to prevent abuses of online services such as registering thousands of free accounts, obtaining tickets for resale, spreading spam emails, taking over accounts by using brute force [2], or perform credential stuffing attacks [3].

The idea of using a CAPTCHA to check whether the users who are making requests to a web service are humans goes back to 1996 [4]. A year later, AltaVista developed the first practical example of a CAPTCHA scheme, which was based on the inability of Optical Character Recognition (OCR) software to recognize a distorted text [5].

In 2000, Von Ahn et al. [6], [7] introduced several practical proposals for designing CAPTCHA schemes based on *hard Artificial Intelligence (AI) problems*, i.e., challenges that most humans can solve easily, but computer programs cannot pass.

Most CAPTCHA schemes proposed in the literature follow such an approach and exploit different elements such as character recognition, image understanding, and speech recognition to create challenges that successfully block automated bots. However, the recent advancement of AI in general and Computer Vision (CV) in particular has made automated programs significantly better at solving such tests. As a result, almost all of the traditional CAPTCHA schemes have been broken as demonstrated in [8], [9], and [10].

Furthermore, in contrast to Von Ahn et al. expectations, not all the attacks proposed in the literature attempt to solve the underlying AI problem on which these CAPTCHAs are based in order to break them. Some of them, instead, try to circumvent the AI problem by leveraging the weaknesses in the design of a particular CAPTCHA scheme [11], [12], [13]. These kinds of attacks are known as side-channel attacks.

Over time, designing effective and user-friendly CAPTCHA schemes based on hard AI problems has become very challenging. This has led to the emergence of a new generation of schemes based on behavioral analysis and sensor readings.

In 2014 Google announced that today's Artificial Intelligence technology can solve even the most difficult variant of distorted text at 99.8% accuracy [14] and moved to a CAPTCHA scheme based on behavioral analysis which is considered the dominant CAPTCHA scheme in the market today. In the academic world, many works have shown the vulnerability of the traditional CAPTCHA schemes, nevertheless, many researchers still aim at breaking traditional CAPTCHA schemes and evaluating their security and usability [15], [16], [17], [18], ignoring the emerging CAPTCHA schemes that have not been broken yet. Still, recent works in the literature do not consider these new CAPTCHA schemes neither in their review nor in their security evaluation [19], [20], [21].

***Contribution**:* In this work, we present an up-to-date comprehensive CAPTCHA survey that includes both the traditional CAPTCHA schemes and the new generation ones, such as those based on behavior and sensor readings, and we propose a novel classification of the existing CAPTCHA literature from 2000 to 2020 based of *ten different groups* (i.e., Text-based, Image-based, Audio-based, Video-based, Game-based, Slider-based, Math-based, Behavior-based, Sensor-based and CAPTCHA for liveliness detection). To the best of our knowledge, this is the first survey that reviews behavioral-based, sensor-based CAPTCHAs, and CAPTCHA designed for

M. Guerar, L. Verderame and A. Merlo are with the Department of Informatics, Bioengineering, Robotics and Systems Engineering, University of Genoa, Italy. E-mail: {name.surname}dibris.unige.it
F. Palmieri is with the Department of Computer Science, University of Salerno, Italy. E-mail: fpalmieri@unisa.it
M. Migliardi is with the Department of Electronic Engineering, University of Padua, Italy. E-mail: mauro.migliardi@unipd.it

liveliness detection in authentication methods. Furthermore, we survey and analyze all the literature regarding the security evaluation of the existing CAPTCHA schemes and the proposed techniques to break them, showing the weaknesses of the different categories of CAPTCHA schemes. This work also allows us to build a timeline for the security of 77 CAPTCHA schemes illustrating the creation and breaking year along with the breaking percentage. Besides showing the evolution of CAPTCHA over two decades, this timeline provides a clear view of the broken CAPTCHA mechanisms and the ones that are worth further investigation. In addition, it elucidates the new design trends in CAPTCHA schemes.

Finally, we discuss the evolution of CAPTCHA schemes in terms of new design trends, their security and their user-friendliness; moreover, we illustrate the open issues, the challenges and the opportunities for further study drawing a roadmap for the design of the next generation of secure and user-friendly CAPTCHA schemes.

Structure: The rest of this paper is organized as follows. In Section II, we introduce a comprehensive classification of conventional and recent emerging CAPTCHA schemes. In Section III, we revise the main attacks against the CAPTCHA schemes described in section II. In Section IV, we provide a discussion on the current state-of-the-art of CAPTCHA, highlighting the CAPTCHA evolution and the limitations of each CAPTCHA design from different standpoints. Section V, discusses open issues, challenges and opportunities for future work. Finally, in Section VI, we draw some conclusions from all the analyses and comparisons performed.

II. CAPTCHA CLASSIFICATION

The traditional classification of CAPTCHA in the literature defines six categories, namely text-based, image-based, audio-based, video-based, math-based and game-based CAPTCHA [22], [23]. However, we consider this classification incomplete because it does not cover the new emerging CAPTCHA schemes. As an example, the most widely adopted CAPTCHA schemes today do not fall into this classification (e.g., reCAPTCHA V2 and Geetest). Nevertheless, even the most recent surveys in the literature adopt this incomplete classification to review and evaluate the security of the existing CAPTCHA schemes [19], [20], [21]. This discrepancy between the relevant literature and the actual state of the art motivated us to propose a more comprehensive classification capable of capturing the new emerging CAPTCHA schemes. We argue that current CAPTCHA schemes can be divided into 10 categories, i.e., *Text-based, Image-based, Audio-based, Video-based, Game-based, Slider-based, Behavior-based, Sensor-based, and CAPTCHAs for liveliness detection in authentication methods*.

It is important to mention that the new CAPTCHA schemes that involve a traditional challenge/response test belong to the old category as well; yet, in order to highlight the development and the new directions in CAPTCHA design, we will focus on the new added mechanisms.

A. *Text-based CAPTCHAs*

Text-based CAPTCHAs are the most popular form of CAPTCHA; in these schemes a text (e.g., a sequence of random characters or words) is distorted and displayed to the user as an image. When words are used, language dependency represents a major limitation of this kind of CAPTCHA schemes. Then, the user is asked to input the text appearing in the image to pass the test. The underlying assumption is that humans can read the distorted text easily, but this is hard for bots using Optical Character Recognition (OCR) techniques.

Since the interaction required to solve the CAPTCHA (i.e., the input of a text) is the same in almost all text-based CAPTCHAs, we classified the variation of Text-based CAPTCHAs according to the different representation of the text of the challenge. Hence, we identified three sub-categories: 1) 2D text-based, 2) 3D text-based, and 3) Animated text-based. Table I gathers all the considered text-based CAPTCHA schemes, a relevant graphical sample, and a detailed description of the challenge.

1) 2D text-based CAPTCHA: The 2D text-based CAPTCHA scheme was initially developed by Andrei Broder and his colleagues at the DEC Systems Research Center in 1997. In the same year, the AltaVista website used such a method to block bots trying to influence the rank of a set of sites on the AltaVista search engine.

In 2000, Von Ahn and Blum, in collaboration with Yahoo, developed **Gimpy CAPTCHA** and **EZ-Gimpy** [24] to prevent spammers from posting malicious advertisements in the chat rooms and to ensure that free accounts were granted only to real individuals. The challenge of the Gimpy CAPTCHA scheme consists of typing correctly at least three out of seven words randomly selected from a dictionary.

EZ-Gimpy is a simplified version of Gimpy showing only a single random word selected from the dictionary. However, the word is rendered to an image using different fonts, background grids and gradients. Furthermore, the image is altered by using blurring, noise and distortion effects on letters.

In 2003, Monica Chew and Henry Baird proposed **Baffle-Text** [25], a text-based CAPTCHA scheme that adopts pseudo-random but pronounceable words along with some masking techniques aiming at preventing the use of OCR software.

In 2010, the popular website for sharing and uploading files **(Megaupload.com)** designed a CAPTCHA scheme based on a new segmentation-resistant mechanism different to that used by **Microsoft**, **Google** and **Yahoo**. This new mechanism relies on the combination of overlapping characters and the "Gestalt Perception" principle which is used to hide some contents of the characters where they connect to each other. The Gestalt Perception principle suggests that humans can reconstruct individual characters mentally, while this task is still difficult for computer programs.

The most widely deployed form of text-based CAPTCHA is the first version of **ReCAPTCHA** [26], which had the two-fold aim of protecting websites from bot attacks and digitize old books. The challenge consists of recognizing two distorted words scanned from old books, one known by the algorithm and one that OCR programs have failed to identify.

The challenge is successfully passed if the user correctly recognizes and types the known word. Besides, if the challenge is passed, the algorithm assumes that the user recognized also the second unknown word.

To improve the usability of text-based CAPTCHAs, Chow et al. [28] introduced the idea of **clickable CAPTCHA**. Their approach consists of combining multiple textual CAPTCHA challenges into a grid of clickable CAPTCHAs (e.g., a 3-by-4 grid). The user has to click on the grid elements that match the challenge requirement. For instance, the challenge can be the identification of English words among non-English words in the grid. Obviously, such a challenge has language dependencies.

In contrast to traditional CAPTCHA schemes that use machine-printed text, authors in [29], [38] proposed **Handwritten CAPTCHAs** that use as challenges synthetic handwritten text images, already known to fool OCR software.

2) 3D text-based CAPTCHA: 3D text-based CAPTCHA schemes exploit the fact that human beings can easily recognize sequences of 3D characters while bot programs cannot; thus, they represent an advancement in comparison to the 2D text-based CAPTCHA schemes.

One of the first proposals is the **Teabag 3D** designed by the OCR Research Team [30] to identify the weaknesses of 2D text-based CAPTCHA schemes and propose a novel – and more secure – CAPTCHA scheme. Teabag 3D consists of an image with a 3D pattern that contains textual characters (as shown in Table I). Thanks to the new CAPTCHA scheme, the authors demonstrated that humans could easily recognize the 3D text and, at the same time, automated systems failed in the recognition task.

Similarly, **Super CAPTCHA** [32] and **3DCAPTCHA** [31] are 3D text-based CAPTCHA schemes that were based on those same assumptions and used on several websites. For instance, Super CAPTCHA is also available as a plug-in for WordPress.org since 2013 [1].

Imsamai and Phimoltares [39] introduced the **3D CAPTCHA** scheme by rendering a sequence of 3D alphanumeric characters and applying a set of different effects to trick automated recognition systems. Those effects include text rotation, text overlapping, noise addition, scaling, font variation, special characters and different background textures.

Recently, Suzi et al. [33] introduced a new type of 3D text-based CAPTCHA, called **DotCHA**. The challenge consists of 3D letters composed of several small spheres. Each character is twisted around a horizontal axis so that each letter is readable at a different rotation angle. Thus, the user needs to rotate the 3D text model multiple times to identify all the letters. From the usability point of view, DotCHA adds an additional task (i.e., the rotation of the model multiple times) in comparison to the traditional text-based CAPTCHAs that require only the input of the text to solve the challenge.

3) Animated text-based CAPTCHA: Animated CAPTCHAs extend text-based schemes by introducing the time dimension. In details, these CAPTCHA schemes animate the textual content in the challenge in a short clip, thus complicating the extraction task for automated systems.

One of the first proposals of animated CAPTCHA has been introduced by Fischer and Herfet [40] in 2006. Their CAPTCHA scheme is based on the idea of projecting the text onto a deforming animated surface. In 2009, Naumann et al. [41] introduced an animated CAPTCHA based on the perception that the human ocular system tends to group different entities that move together. Hence, the authors developed a new CAPTCHA scheme that shows letters superimposed over a noisy background. The users are able to distinguish the text from the background when the letters are moving.

Similarly, Cui et al. [42] proposed an animated CAPTCHA where the user can get the right characters shown in the animation only when they are moving. They also introduced the "zero-knowledge per frame" principle, which ensures that each frame of the animation does not leak enough information to solve the CAPTCHA challenge.

Besides the CAPTCHA schemes proposed by the scientific community, there are a set of solutions offered either by specific websites or by CAPTCHA service providers.

For instance, the Creo Group [36] introduced in 2010 an animated CAPTCHA, called **HelloCAPTCHA**, freely available through the developers' website. In general, the HelloCAPTCHA challenge consists of a sequence of six characters presented in an animated GIF image. In some challenges, the characters change position and orientation, and in others, they are not all visible at the same time. The idea behind such a scheme is to spread the information over multiple animation frames to prevent a typical OCR attack over a single frame. **NuCaptcha** is another animated CAPTCHA scheme [37]. The challenge consists of a video with scrolling text in white font, followed by three random red characters moving across a dynamic background. The user is required to type the moving red characters to solve the CAPTCHA. **Dracon CAPTCHAs** [34] are animated visual Flash CAPTCHAs. The challenge consists of recognizing five characters displayed at fixed locations and randomly altered by using fade and blur effects. The animation is enriched with noise, e.g., random falling bars in the foreground or small text characters in the background. **KillBot Professional** version [35] is a commercial animated CAPTCHA that claimed among its client the United States Federal Government. In detail, the users have to recognize five moving characters displayed in a noisy foreground and background that are composed of lighter colors than the main text characters. **Atlantis CAPTCHA** [35] is an animated CAPTCHA used on the Atlantis website[2]. In such a CAPTCHA, users need to recognize six moving characters among others that are continuously changing their color.

B. *Image-based CAPTCHAs*

An alternative to text-based CAPTCHA schemes are image-based ones. In these schemes, the challenge presented to

[1] https://wordpress.org/plugins/super-capcha/#description

[2] Atlantis-caps.com

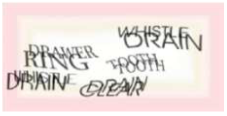
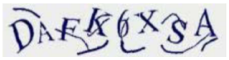
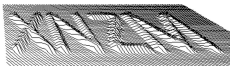
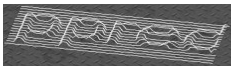
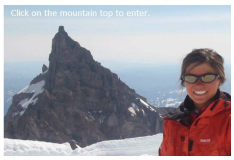
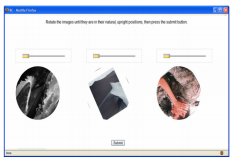
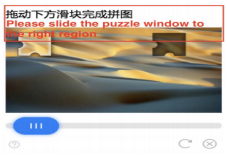
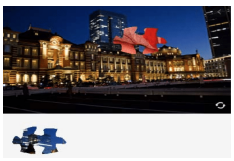
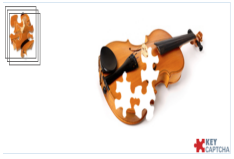
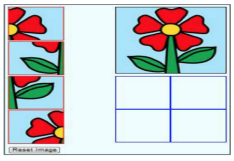
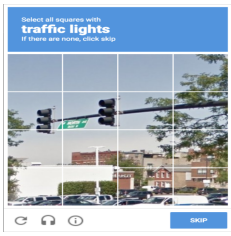
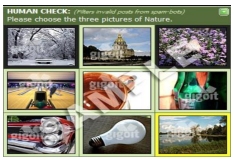
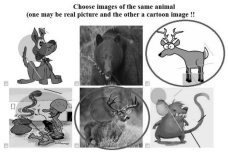
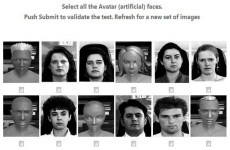
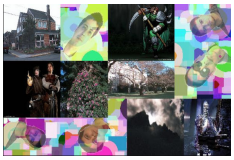
Type	Scheme	Sample	Year	Challenge Description
2D	GIMPY [24]		2000	Recognize three words out of of seven selected randomly from a dictionary
	EZ-GIMPY [24]		2000	Recognize one English word in a distorted image
	BaffelText [25]		2003	Recognize a pronounceable string of characters with difference masking applied.
	Microsoft (MSN) [27]		2002	Recognize eight distorted characters presented with random arcs as clutters.
	Google (Gmail) [27]		2006	Recognize characters which are crowded together
	Yahoo [27]		2008	Recognize a string of characters connected by intersecting random lines
	Megaupload		2010	Recognize four overlapped characters with negative intersection areas
	ReCAPTCHA V1 [26]		2008	Recognize distorted text scanned from old books.
	Clickable CAPTCHA [28]		2008	Identify English words among non-English words
	Handwritten [29]		2004	Recognize a distorted handwritten text (e.g., city name).
3D	Teabag 3D [30]		2006	Recognize a sequence of characters that appears on a grid in 3D space
	3DCAPTCHA [31]		2006	Recognize a sequence of 3D characters
	Super CAPTCHA [32]		2013	Recognize a sequence of 3D characters
	DotCHA [33]		2019	Drag and rotate the model to identify each letter, then type the answer
Animated	Dracon CAPTCHA [34]		2006	Recognize five characters which fade and blur at various times over the animation frames
	KillBot Professional [35]			Recognize five moving characters among a noisy foreground and/or background.
	Atlantis CAPTCHA [35]			Recognize six moving characters among other continuously changing their color.
	HelloCAPTCHA [36]		2010	Recognize a sequence of six characters displayed in an animated GIF image.
	NuCaptcha [37]		2008	Type the last three red moving characters.

TABLE I: A taxonomy of text-based CAPTCHAs

the user is generally based on understanding a written text describing a task that needs an additional image classification or recognition task to be completed. The textual part has language dependencies. The user interaction or the gesture required to solve the challenge may differ from a scheme to another, therefore, we suggested a classification based on those differences, identifying six different types, as shown in Table II and described in the following.

Type	Scheme	Sample	Year	Challenge Description
Click	Implicit CAPTCHA [43]		2005	Click on a specific area of an image (e.g., mountain top)
	SACaptcha [44]		2018	Click on some regions in the image that have a specific shape mentioned in the challenge description
Sliding	WHAT'S UP CAPTCHA [45]		2009	Move the slider to adjust at least three randomly rotated images to their upright orientation.
	MintEye CAPTCHA [46]		2012	Move the slider until undistorted version of the image appears
	Tencent (Tencent.com)			Drag the slider until two puzzle pieces match.
Drag and Drop	Garb CAPTCHA [47]		2013	Drag and drop the puzzle pieces to their correct position to reconstruct the original image.
	Capy CAPTCHA [48]		2012	Drag a puzzle piece to complete a jig-saw
	KeyCAPTCHA [49]		2010	Drag three puzzle pieces to assemble the image
	Gao et al [50]		2010	Identify the two misplaced pieces and swap them
	Hamid Ali et al [51]		2014	Drag and drop four images to an empty grid following the same order in the reference image.

Type	Scheme	Sample	Year	Challenge Description
Selection	Asirra [52]		2007	Select cats from a set of 12 images of cats and dogs
	No CAPTCHA reCAPTCHA [14]		2014	Select images that have the same content described in the challenge with a sample image.
			2014	Select all images with street signs, cars, bridges or some specific object.
	Facebook image CAPTCHA			Select the images that correspond to a hint from twelve images with different content.
	HumanAuth [53]		2006	Select images with natural contents.
	SEMAGE [54]		2011	Select semantically related images from a set of images.
	AVATAR [55]		2012	Select avatar faces from a set of 12 images composed of a mix of human and avatar faces
	FR-CAPTCHA [56]		2014	Select real human faces distorted among nonhuman face images.
	FaceDCAPTCHA [57]		2014	Select two face images of the same person.

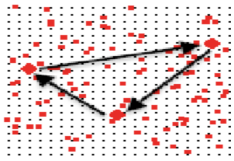
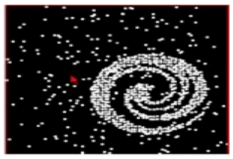
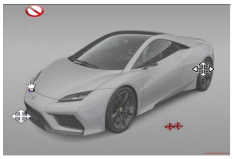
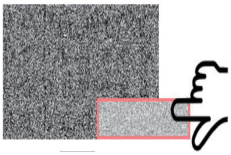
Type	Scheme	Sample	Year	Challenge Description
Drawing	VAPTCHA [58]		2018	Draw an resemblant trajectory to match the reference trajectory
	Drawing CAPTCHA [59]		2006	Connect a specific dots to each other
	MotionCAPTCHA [60]		2011	Draw a shape displayed in a box
Interactive	CAPTCHAStar		2015	Move the cursor until forming a recognizable shape
	Cursor CAPTCHA [61]		2013	Overlap the cursor on the identical object placed in a random generated image
	Noise CAPTCHA [62]		2012	Move a small noisy image over a large noisy image until a hidden message or object appears

TABLE II: A taxonomy of image-based CAPTCHAs

1) Click-based CAPTCHAs: This type of scheme shows an image and a text that explains where the user needs to click to complete the challenge. A typical example is **Implicit CAPTCHA** [43], where the users are required to click on a specific static place on an image according to the given instruction, e.g., "Click on the climber's glasses" or "Click on the logo on the climber's arm".

The major limitation of such a CAPTCHA scheme is that the challenge cannot be generated automatically, and thus it requires the human intervention to generate a new instance. Recently, a new image-based CAPTCHA, called **SACaptcha**, has been introduced by Tang et al. [44]. Users are required to click on some regions in the image that have a specific shape mentioned in the challenge description to pass the CAPTCHA test.

2) Sliding image-based CAPTCHAs: In sliding image-based CAPTCHAs, users are required to use the slider to solve an image-based challenge such as adjusting the orientation of an image, selecting the correct form of an image, or moving a fragment of an image to the correct location.

For instance, **WHAT's Up CAPTCHA** [45] presents three randomly rotated images to the users and asks them to use the slider to rotate the images to their upright position. The success rate of a random guess depends on the tolerance of accepted answers. According to the data reported in [45], the success rate of a random guess on one image is 4.48%, but it decreases to 0.009% for three images. Slide-to-fit CAPTCHA [46] by **Minteye** presents a distorted image through a swirl filter with a small slider below the image. Users have to move the slider until the user sees the undistorted version of the image. **Tencent CAPTCHA** asks the users to drag the slider until two puzzle pieces match. One of these puzzle pieces represents the target region in the image, where the users have to place the other piece of the puzzle to have a complete image.

3) Drag and drop based CAPTCHAs: The Drag and drop CAPTCHA scheme requires the users to combine or reorder image pieces by dragging and dropping them to form a complete picture.

For instance, **Garb CAPTCHA** [47] presents an image divided into four pieces randomly shuffled. To pass the CAPTCHA test, users have to reorder them to reconstruct the original image. Similarly, **Hamid Ali et al.** [51] introduced a puzzle-based CAPTCHA. The challenge consists of dragging and dropping four images or pieces of the same image into an empty grid of four cells. To pass the CAPTCHA test, the position of each image in the grid should be the same as in the reference image. **Gao et al.** [50] proposed an image-based CAPTCHA that uses the Jigsaw puzzle. Their CAPTCHA displays an image divided into pieces (i.e., 9, 16, or 25 depending on security level), but only two are not in the original positions. Users have to identify the two pieces and drag one over the other to swap them to solve the puzzle. **Capy CAPTCHA** [48] asks the users to drag one puzzle piece into the correct location within the challenge image. The puzzle void is filled with a fraction from the same or another image rather than a random color. **KeyCAPTCHA** [49] shows an incomplete image along with three puzzle pieces and asks the users to assemble the image as they see it in the reference image displayed in the upper right corner of the frame. The reference image is shown with a small resolution, and it disappears once the cursor is inside the frame. To pass the CAPTCHA test, the users have to drag and drop the three puzzle pieces in their correct position.

4) Selection-based CAPTCHAs: Selection-based CAPTCHA schemes ask users to select candidate images from sets of images. The task can be described with text only or with text and a sample image.

A typical CAPTCHA of this kind is **Asirra** [52], which displays 12 images of cats and dogs and asks users to select all cat images among them. Similarly, **HumanAuth CAPTCHA** [53] asks the users to select all images with natural content. It is based on humans' ability to distinguish between images with natural content (e.g., tree, river) and artificial one (e.g., car, watch). In contrast to Asirra and HumanAuth CAPTCHA, **SEMAGE** (SEmantically MAtching imaGEs) CAPTCHA [54] asks users to select semantically related images from a given image set. Thus, the user is required to recognize the content of each image and then understand and identify the semantic relationship between a subset of them.

In 2014, Google introduced the second version of re-CAPTCHA based on behavior analysis, called **"No captcha reCAPTCHA"** [14], [63]. In this version the system analyzes the browser environment (e.g., browser history, cookies, etc.) and evaluate the risk of being confronted with a bot; if the risk is considered high, then the page displays a selection-based CAPTCHA, otherwise checking a checkbox is enough. The selection-based CAPTCHA challenge consists of a sample image with a keyword describing the content of the image and 9 candidate images. The user is required to select images that are similar to the sample to pass the challenge.

Facebook's image CAPTCHA follows the same approach of reCAPTCHA except for the sample image. To pass the challenge, users have to select the images that correspond to the description (i.e., hint) from twelve images with different content. Afterward, Google introduced other variations of image-based reCAPTCHA that ask the user to select images with vehicles, houses, street signs, or other specific objects.

Among others, several selection-based CAPTCHAs rely on face images for their challenges. For instance, **Avatar CAPTCHA** [55] requires users to choose avatar faces from a set of 12 grayscale images composed of a mix of human and avatar faces. Other face-based image CAPTCHAs are **FR-CAPTCHA** [56] and **FaceDCAPTCHA** [57]. FR-CAPTCHA asks users to select two face images of the same person displayed in a complex background. Differently, FaceDCAPTCHA requires users to identify the visually distorted real human faces among nonhuman face images. Unlike Avatar, the human face images used in FR-CAPTCHA and FaceDCAPTCHA are rotated, distorted, or embedded in a complex background.

5) Drawing-based CAPTCHAs: The CAPTCHAs schemes belonging to this category distinguish computers and human beings thanks to a drawing challenge.

Shirali-Shahreza has introduced the first drawing-based CAPTCHA, named **Drawing CAPTCHA** in 2006 [59]. Users are required to draw lines to connect diamond-shaped dots.

These dots are displayed on a screen with noisy background, so users have to identify them first. Another CAPTCHA that falls into this category is **VAPTCHA** (Variation Analysis-Based Public Turing Test to Tell Computers and Humans Apart) [58]. The VAPTCHA challenge consists of an image containing a randomly generated reference trajectory. Users are required to draw a resemblant trajectory to match the reference trajectory to complete the verification. If the matching degree is equal to or higher than the minimal match degree defined by the system, users are classified as humans, otherwise they are assumed to be bots. Similarly, **MotionCAPTCHA** [60] asks users to draw a shape similar to the one displayed in the challenge box.

6) Interactive-based CAPTCHA: CAPTCHA schemes in this category rely on the user's interaction through mouse movement or swiping gesture to discover a secret position in an image. This position represents the answer to the challenge and it is revealed only after the user's interaction.

For instance, Conti et al. [64] proposed a new CAPTCHA scheme, called **CAPTCHaStar**. The proposed CAPTCHA leverages the human ability to recognize shapes in a confusing environment. The underlying assumption is that a machine cannot easily emulate this ability. The CAPTCHaStar challenge consists of white pixels, called stars, randomly mixed during the generation of the challenge. The position of these stars changes according to the position of the cursor. To pass the CAPTCHA test, users have to move the cursor until the stars aggregate in a recognizable shape, then, click on the left mouse button to send the cursor coordinates to the server. If the cursor is close to the secret position, users are considered as humans. On mobile devices, CAPTCHaStar requires swiping the fingers to move the cursor and tapping the "check" link to submit the final answer.

Similarly, Okada et al. [62] introduced **Noise CAPTCHA**, which is composed of two noisy images with different sizes and a hidden object or message in a specific position in the image. To pass the CAPTCHA test, users have to move the small noisy image over the large image until the hidden object appears, then click on the "submit" button. Similar to CAPTCHaStar, users are considered as humans when they identify the correct (secret) position at which the object or the image becomes visible.

Thomas et al. [61] propose **Cursor CAPTCHA**, which displays five cursor images in a randomly generated image and customizes the cursor image of the mouse pointer. Then, the CAPTCHA asks users to overlap the mouse pointer on an identical cursor image to pass the challenge. At the beginning of the test, users see six cursor images in which two of them are identical, but they are unable to identify the target position until they move the mouse.

C. *Audio-based CAPTCHAs*

Audio-based CAPTCHA schemes were initially proposed as an alternative to visual CAPTCHAs for people who have a visual impairment. To pass the test, they are required to type what they have heard.

One of the most popular audio-based CAPTCHA was the **audio reCAPTCHA** proposed by researchers at Carnegie Mellon University and later acquired by Google. To pass the CAPTCHA challenge, users have to recognize eight spoken digits with a background noise composed of human voices speaking backward at varying volumes. Audio reCAPTCHA accepts only one mistake in one of the digits to solve the challenge.

Nevertheless, Sauer et al. [65] showed that this CAPTCHA scheme represents a hard task for blind users. Indeed, their usability study involving six blind participants shows that the participants were able to complete only 46% of the tasks correctly.

Similarly, many popular websites implement audio CAPTCHAs that rely on listening to a random sequence of digits. For instance, **e-Bay Audio CAPTCHA** consists of six digits spoken in different voices with regular background noise. **Microsoft CAPTCHAs** are composed of ten digits spoken in different voices with regular background noise consisting of several simultaneous conversations. **Yahoo CAPTCHA** asks the users to type seven digits that follow three beeps spoken by a child with background noise consisting of other children's voices. The **Audio reCAPTCHA** version used in 2013, asks the users to identify all digits presented in the challenge composed of three clusters. Each cluster contains three or four overlapping digits. In 2017, Google released a new version of **reCAPTCHA** with ten spoken digits and background noise. The available experiences of Audio-based CAPTCHAs are summarized in table III.

D. *Video-based CAPTCHAs*

CAPTCHA schemes in this category reproduce a short video and then propose a textually described challenge that requires some level of comprehension of the video content.

For instance, **Kluever et al.** [66] proposed a CAPTCHA that asks the user to watch a video and provide three words that best describe the video. Similarly, Shirali-Shahreza et al. proposed **Motion captcha** [67] that asks the users to watch a video, then they have to select the sentence that describes the motion of the person in the video.

The most common implementations of Video-based CAPTCHAs are reported in table III.

E. *Math-based CAPTCHAs*

CAPTCHA schemes in this category ask the users to solve a challenge based on a mathematical problem.

A typical example of Math-based CAPTCHA is **Arithmetic CAPTCHA** that relies on basic arithmetic operations such as (+,*,-). To solve the challenge, users have to enter the results of a simple math operation such as "2+1= " to prove that they are human. Unlike Arithmetic CAPTCHA, **QRBGS CAPTCHA** [68] usually asks the users to solve a complex equation that involves trigonometric and differential functions. The main problem with such kind of CAPTCHAs is that it assumes that all users have advanced knowledge in mathematics, and it requires a long time to solve the challenge.

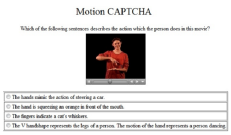
Captcha Type	Captcha Scheme	Sample	Year	Challenge Description
Video-based	Kluever el al [66]		2009	Watch a video and provide three words that best describe the video
	Motion captcha [67]		2008	Select the sentence that describes the motion of the person in the video
Audio-based	Audio ReCAPTCHA (non-continous)		2008	Recognize eight spoken digits with background noise consisting of human voices speaking backwards at varying volumes
	e-Bay audio CAPTCHA			Recognize six digits spoken in different voices with regular background noise
	Microsoft CAPTCHA			Recognize ten digits spoken in different voices with regular background noise consisting of several simultaneous conversations
	Yahoo CAPTCHA			Recognize seven digits that follow three beeps spoken by a child with background noise consisting of other children's voices
	Audio reCAPTCHA (Continuous)		2013	Identify all digits presented in the challenge that consist of three clusters and each cluster contains three or four overlapping digits.
	Audio ReCAPTCHA (version 2017)		2017	Recognize ten spoken digits with background noise

TABLE III: A taxonomy of video and audio-based CAPTCHAs

F. Slider CAPTCHAs

Slider CAPTCHA is another type of CAPTCHA scheme that relies only on the sliding gesture. Unlike sliding image-based CAPTCHAs previously described, image recognition is not part of the challenge. Users have only to move the slider across the screen to prove they are human.

For instance, the CAPTCHA used by **Taobao.com**, which is a Chinese online shopping website owned by Alibaba, asks the users to drag the slider from the start to the end of the sliding bar to verify whether they are human or not. Similarly, CAPTCHA used by **TheyMakeApps.com** asks the users to move the slider to the end of the line to submit a form [69]. This type of CAPTCHA has been widely adopted due to its ease of use.

Some well known examples of Math and Slider-based CAPTCHAs are reported in table IV.

G. Game-based CAPTCHAs

Game-based CAPTCHA schemes have emerged as an alternative that tries to make the task of solving CAPTCHAs a fun activity for the users. These CAPTCHAs are based on the assumption that humans – unlike automated systems – can understand the rules of a game and solve the challenge. Users are required to solve a straightforward game that is often based on image semantics. There are also attempts to make the users enjoy solving math-based CAPTCHAs by offering games such as tic-tac-toe and a dynamic roll-dice game.

A well-known game-based CAPTCHA is **PlayThru CAPTCHA** [70] designed by a startup called "Are you a human". The challenge requires moving some dynamic objects that have a semantic connection with the static target image. For instance, users might be asked to place food in the refrigerator or feed a baby. Mohamed et al. [71] developed four **Dynamic Cognitive Games (DCG)** similar to PlayThru, in order to investigate both its security and usability. Depending on the game, users are required to drag and drop dynamic objects to match them with others (e.g., match objects with similar shapes) or place them in specific regions (e.g., place the ships on the sea). Their usability study shows that all the four games last less than 10 seconds, and all the participants successfully completed the games within the time out. Regarding the error rate per drag and drop, the authors noticed that the visual matching tasks are less error-prone than the semantic matching tasks.

Another example of game-based CAPTCHA is **Sweet-CAPTCHA**. Also in this case, the users are required to drag and drop an image with a semantic connection with the target image. For example, users need to drag milk to a cup of coffee, drag the player to the guitar, or drag chopsticks to sushi. Another example is **Tic Tac Toe CAPTCHA** that proposes to

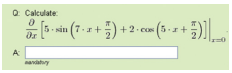
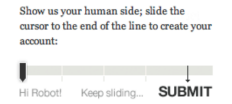
Captcha Type	Captcha Scheme	Sample	Year	Challenge Description
Math-based	Arithmetic CAPTCHA			Enter the result of the math operation
	QRBGS CAPTCHA [68]		2008	Enter the result of a complex mathematical equation.
Slider-based	Taobao			Drag a slider from the start to the end of the sliding bar
	TheyMakeApps CAPTCHA [69]		2010	Move the slider to the end of the line.

TABLE IV: A taxonomy of Math and slider-based CAPTCHAs

the user an almost complete the tic-tac-toe game, where users need a single move to win the game and get 3 Xs in a row.

Some CAPTCHA designers have tried to have users having fun when they solve CAPTCHAs based on a mathematical problem. A typical example is **Dice CAPTCHA** (i.e., Homosapiens Dice version) [72], where users are required to roll some dice and then compute the sum of the digits appearing on them. If the entered sum is correct, the users are considered humans.

A detailed taxonomy of the most common game-based CAPTCHAs is reported in table V.

H. Behavior-based CAPTCHAs

CAPTCHA schemes in this category employ behavioral biometrics such as keystroke dynamics, mouse dynamics, swipe dynamics, and eye movement to distinguish between humans and bots. Most of the proposed schemes involve mouse/swipe dynamics with conventional CAPTCHA schemes (e.g., image-based or game-based).

As an example, Acien el al. [73] proposed in 2020 **BeCAPTCHA-Mouse**, which asks the user to solve an image-based CAPTCHA similar to reCAPTCHA V2. However, such a scheme analyzes the mouse trajectories performed during the task to distinguish between humans and bots. Similarly, **Gametrics** [74] asks the users to solve a Dynamic Cognitive Game CAPTCHA. During the drag and drop operations requested to solve the challenge, the CAPTCHA collects the mouse movement features to distinguish between human and automated systems.

In addition, **GEETest** and **Netease** [75] ask the users to solve a sliding image-based CAPTCHA similar to Tencent CAPTCHA. In detail, the users need to complete an image by dragging the slider to match two puzzle pieces (one reflecting the missing part of the image, the other the correct position in the image). Unlike Tencent CAPTCHA, users are considered humans only when both the puzzle pieces match and the sliding behavior is not considered suspicious.

Furthermore, the same authors of BeCAPTCHA-Mouse proposed a variation for smartphones called **Be-CAPTCHA** [76] that is based on a slider challenge. However, unlike traditional sliding tasks, the algorithm leverages swiping gestures and sensor data to detect human behavior.

Siripitakchai et al. [77] proposed **EYE-CAPTCHA**, which asks the users to solve a math-based CAPTCHA relying on the eye movement. In detail, the challenge prompts a simple math operation in the center on the screen, along with four potential answers at the corners. To solve the challenge, the user has to locate the right answer and move it through his eyes to the center.

Unlike the above-mentioned behavioral CAPTCHAs, the **"No CAPTCHA reCAPTCHA"** (a.k.a., reCAPTCHA V2) deployed by Google in 2014 does not use a traditional CAPTCHA scheme to gather information on the user behavior. On the contrary it only requires to click on the "I'm not a robot" Checkbox. However, in the background, information related to user's behavior (e.g., the mouse movement, where the users click, how long they linger over a checkbox) along with other information such as the installed plugins, the language of the browser and cookies are collected and analyzed by an engine that evaluates the risk of being confronted with a bot. If the user is classified as human, no additional tasks are required. Otherwise, the system prompts a traditional image-based reCAPTCHA as a second security layer.

In 2017, Google released another variation of reCAPTCHA V2, called **Invisible reCAPTCHA**. As its name suggests, the challenge is invisible to the user. The verification process is performed in the background, and it is invoked when the user clicks on an existing button on the web page or by a JavaScript API call. Similarly to the "No CAPTCHA reCAPTCHA" approach, Invisible reCAPTCHA requires to solve the traditional image-based reCAPTCHA if and only if the risk analysis engine cannot recognize a human behavior with a given level of confidence.

A detailed taxonomy of the most common behavior-based CAPTCHAs is reported in table VI.

I. Sensor-based CAPTCHAs

The CAPTCHA schemes belonging to this category rely on the data gathered by one or more hardware sensors. These CAPTCHA schemes are typically designed for mobile devices that natively host sensors like gyroscope or accelerometer.

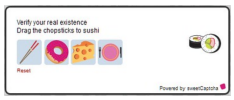
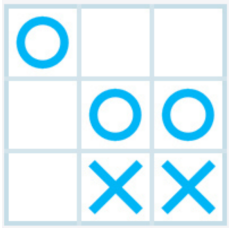
Captcha Scheme	Sample	Year	Challenge Description
PlayThru [70]		2012	Play a simple game that consist of moving specific dynamic objects to a specific place according to the image semantics.
DCG CAPTCHAs [71]		2014	Depending on the challenge description, Drag and drop objects to match them with others or place them in specific regions.
SweetCAPTCHA		2011	Drag specific static images to match them with the target image.
Dice CAPTCHA [72]		2010	Click on "Roll" to roll the dices, then enter the sum of the numbers appearing on the dices.
Tic tac toe CAPTCHA		2011	Complete the game by tapping into the correct position to get a line of 3 Xs (or Os)

TABLE V: A taxonomy of game-based CAPTCHAs

Sensors-based CAPTCHA schemes can be further divided into *physical* and *cognitive*. In the first case, the sensors' data are used to discriminate between a human and a bot. In the latter, the sensors only provide an input channel for the actions of the user.

A detailed taxonomy of the common available sensor-based CAPTCHA experiences is reported in table VII.

1) Physical CAPTCHAs: The first physical CAPTCHA for mobile devices has been introduced by Guerar et al. [78] in 2015. The proposed CAPTCHA scheme, called **CAPPCHA** (Completely Automated Public Physical test to tell Computers and Humans Apart) or **TiltToGo**, requires the users to tilt the device to a specific degree to prove they are humans. The challenge exploits the impossibility for a software bot to perform a physical task such as moving the device. Furthermore, thanks to the use of dedicated hardware sensors, the CAPTCHA scheme does not require randomizing the challenge or executing sophisticated gestures. Therefore, the authors suggested a simple gesture such as tilting the device to a specific degree, which can be detected easily through motion sensors such as the accelerometer and gyroscope.

Similarly, in 2016, Hupperich el al. [79] proposed **Sensor CAPTCHA** that asks the users to move the device to prove they are humans. Unlike CAPPCHA, Sensor CAPTCHA asks the users to perform a complex gesture such as hammering, fishing, drinking, or turning the body while holding the mobile device.

In [80], the authors suggested **Pedometric CAPTCHA** that requires walking at least five steps to be considered humans. The idea behind this is to create an acceleration in the mobile device while the user is walking that cannot be generated by a bot. **Mantri et al.** [81] proposed a CAPTCHA scheme that asks the users to move the device according to a specific pattern displayed on the screen. For instance, the user is required to write an "S" letter while holding the device and then press the "submit" button. Similarly, **Frank et al.** [82] asks the users to move the device to perform a gesture that can be detected by the gyroscope, such as tilting the device, rotating the device or drawing a three-dimensional shape or letter while holding the device.

In [83], Guerar et al. proposed **Invisible CAPPCHA** based on the same idea of CAPPCHA, although - as the name suggests - the challenge is invisible to the users. The authors noticed that most of the online services that require protection against automation abuses in mobile devices require the interaction with the touchscreen (e.g., fill a form, write a comment, tap on a button, perform the login). Such physical interactions cause micro-movements of the device that can be tracked by motion sensors such as the accelerometer. Based on their observation, they leveraged the implicit user's taps to make the challenge transparent to the users and thus more user-friendly. Unlike the Invisible reCAPTCHA designed by Google, Invisible CAPPCHA is based on humans' ability to perform a physical task and not on the way they perform the task. Also, the tap gesture is detected through sensors readings rather than touchscreen events that can be easily simulated by the bots [1]. Furthermore, no sensitive data are provided to the server side as the interpretation of the sensor data is completely performed inside trusted hardware in the client side and thus it preserves the user's privacy.

2) Cognitive sensor-based CAPTCHAs: Similar to the traditional CAPTCHAs, Cognitive sensor-based CAPTCHAs ask the users to solve a cognitive challenge (e.g., recognizing an

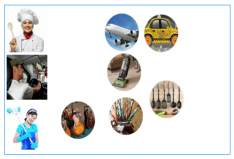
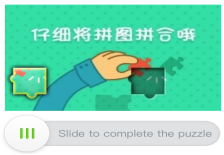
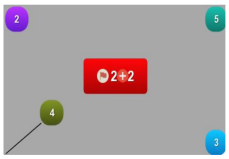
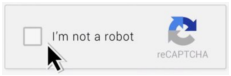
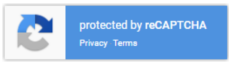
CAPTCHA Scheme	Sample	Year	Challenge Description
BeCAPTCHA-Mouse [74]		2020	Solve a selection image-based CAPTCHA.
Gametrics [74]		2016	Drag-drop a subset of the moving objects to their orresponding targets which are static.
GEETest (geetest.com)		2012	Drag the slider until two puzzle pieces match.
Netease [75]			Drag the slider until two puzzle pieces match.
Be-CAPTCHA [76]		2020	Drag a slider from the start to the end of the sliding bar
Eye-CAPTCHA [77]		2017	User locates the answer of a simple math operation displayed in the screen and move it using his eyes to the center.
No CAPTCHA reCAPTCHA [63]		2014	Click on I'm not a robot Checkbox
Invisible reCAPTCHA [63]		2017	No visible challenge, it is invoked via a Javascript API or when the user clicks on an existing button on the website.

TABLE VI: A taxonomy of behavior-based CAPTCHAs

image, or solving a game), yet they use sensors as their input to solve the challenge rather than the conventional taping or swiping gestures. To this aim, we classified these CAPTCHAs as sensor-based CAPTCHA rather than including them in one of the categories mentioned above to highlight the current research trends.

A typical example of this category is **AccCAPTCHA** [84], where the challenge requires to play a simple game such as the rolling ball game. Thanks to the device's motion sensors, the user can move the ball to complete the game.

Yang et al [85] proposed **GISCHA**, a game-based image semantic CAPTCHA for mobile devices. The challenge consists of a rolling ball and destination holes with different shapes. The direction of the rolling ball can be controlled by turning the mobile device to different angles. The users are considered as human if they successfully move the ball to the destination hole shaped like a circle. Similarly, the CAPTCHA designed by **Ababtain el al.** [86] asks the users to solve a simple game to prove that they are humans, also in this case, using the sensors as their input. They suggested five games where all of them use one dynamic object and one or multiple static objects. To pass the test, the users have to move the dynamic object, so that it touches specific static objects which are considered as targets.

Recently, Feng el al. [84] proposed **SenCAPTCHA** that is based on the difficulty of finding an animal facial key point. Such a CAPTCHA scheme proposes an image of an animal along with a small red ball. The users are required to tilt their devices to move the red ball into the center of that animal's eye. The idea behind using the sensor readings is to avoid the traditional input modalities (i.e., typing, selecting images) that can be inconvenient on devices with small screen sizes.

J. CAPTCHAs for liveliness detection in authentication methods

Today, one of the biggest problems that threats every website with a login is the use of malicious bots for credential stuffing and credential cracking. This is due to the availability of billions of breached credentials. Imperva [87] reported that a recent credential stuffing attack lasted 60 hours and included 44 million login attempts. In the literature, there are many proposals that attempt to embed a form of CAPTCHA in the authentication methods to stop these attacks.

In 2010, Stefan Popoveniuc [88] proposed an authentication method called SpeakUP, for remote unsupervised voting. They added text-based CAPTCHA to voice biometrics. To log in, the voters are required to read out loud a 2D text CAPTCHA displayed on the screen that is associated with the candidate for whom they wish to vote. The voters are identified by the biometric characteristics of their voices. For further security, the author suggested to capture a video of the voter while solving the CAPTCHA.

Recently, Uzun el al. [89] proposed a Real Time CAPTCHA system called rtCaptcha for defending against automated attacks on facial authentication systems. Similar to SpeakUp CAPTCHA, once the authentication session start, users are required to take a video while pronouncing out loud the 2D text CAPTCHA presented as a challenge to prove they are humans. The session will time out if no response is received after a predefined period.

In [90], authors proposed BrightPass, an authentication method for mobile social media networks. They added liveliness detection mechanism to PIN/password in order to prevent the automated process of iterating through the entire password space and from testing all the stolen passwords. Their proposed mechanism leverages screen brightness, which cannot be captured by malicious programs, to tell the users when to input a correct PIN digit and when to input a misleading lie digit.

In [91], [92], authors proposed a PIN-based authentication method for smartwatches that embeds a form of physical CAPTCHA. This mechanism uses the same principle behind CAPPCHA [93]. Users have to physically rotate the bezel to a specific degree to input the PIN digits. Using a trusted hardware (i.e., the bezel) this mechanism prevents any automated program from performing a brute force or credential stuffing attacks. This mechanism can be also used separately from PIN-based authentication. Similarly, authors in [94] leverage the rotation of the smartwatch digital crown to prevent automated attacks against the PIN code.

III. Security of CAPTCHA schemes

The different proposals of CAPTCHA schemes aim to discern between human and computing systems thanks to a challenge. Instead, from an attacker perspective, the goal is to break the CAPTCHA scheme, i.e., to solve the proposed challenge with an automated system and still being recognized as a human.

The general process of breaking CAPTCHAs can be divided into the following phases/stages: pre-processing, segmentation, and recognition. Pre-processing techniques (e.g., image binarization, image thinning, and noise removal) are usually used to remove background patterns, separate the foreground from the background, and eliminate noise before the segmentation and recognition phases [96]. In some cases, extraction techniques are used before pre-processing [97], such as Pixel Delay Map (PDM), Catching Line (CL), and Frame Selection (FS).

Many efforts have been put into breaking the different CAPTCHAs by the scientific community in the last years. To do so, attackers can rely on a set of attacking methodologies that can be grouped in:

- **Object Segmentation Attacks.** In this category, segmentation techniques are used to split the CAPTCHA image into segments that contain individual objects to facilitate recognition. Well-known techniques that have been used in breaking CAPTCHAs are vertical histogram, color-filling, snake segmentation [96], and JSEG.
- **Object recognition attacks.** This type of attack includes object recognition attacks, pixel-count, dictionary and database attacks [96]. The common techniques used for object recognition are pattern matching (e.g., shape context matching [98], correlation algorithm [99]), OCR recognition, Scale-Invariant Feature Transform (SIFT) and machine learning.
- **Random Guess Attacks.** In this type of attack, attackers try to break the CAPTCHA scheme by guessing the correct answer. Therefore, CAPTCHAs with a small number of different challenges are vulnerable to this attack.
- **Human Solver Relay Attacks.** The bot forwards the CAPTCHA challenges to remote human workers to solve the CAPTCHAs in exchange for a small income. The human workers solve the challenges and send the correct responses to the bot that can solve the CAPTCHA accordingly.

In the following we outline the existing techniques for attacking the different types of CAPTCHA schemes presented in section 2. Furthermore, we plot them in a timeline graph (Figure 1) to detail the number of years that occurred to break each CAPTCHA scheme and the best breaking percentage achieved. As shown in the graph, most of the traditional CAPTCHAs have been broken, including the No CAPTCHA reCAPTCHA scheme.

A. Attacks against text-based CAPTCHA

A lot of works suggested methods to break the different type of text-based CAPTCHAs. In 2003, Mori and Malik [98] proposed a method based on shape context matching to break both Gimpy and EZ-Gimpy CAPTCHAs with 33% and 92% accuracy, respectively. In [99], EZ-Gimpy was also broken with a success rate of 99% using a correlation algorithm and a direct distortion estimation algorithm. In 2005, Chellapilla et al. [100], [101] were able to break various text-based CAPTCHAs by using machine learning, and suggested a secure CAPTCHA scheme based on hard-segmentation problems. In 2008, Yan and El Ahmad showed that some segmentation-resistant CAPTCHAs could be broken, including the ones used by Microsoft, Google, and Yahoo [27], [102]. El Ahmad and Yan [103] were able to break Megaupload CAPTCHA with a success rate of 78%. In 2014, researchers

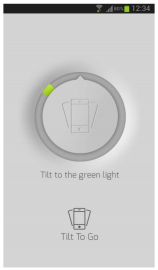
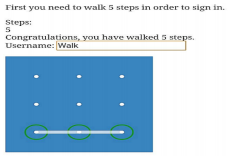
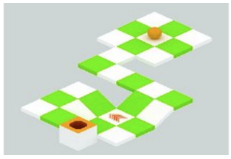
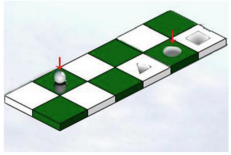
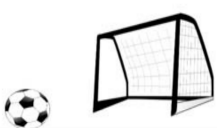
CAPTCHA Type	CAPTCHA Scheme	Sample	Year	Challenge Description
Physical	CAPPCHA (TiltToGo) [78]		2015	Tilt the device to a specific degree
	Pedometric CAPTCHA [80]		2017	Walk at least 5 steps
	Mantri et al. [81]		2017	Move the device according to a specified pattern displayed on the screen.
	Sensor CAPTCHA [79]		2016	Perform gestures such as hammering, fishing, turning the body while holding the mobile device.
	Invisible CAPPCHA [83]		2018	No task is required
	Frank et al. [82]		2018	Move the device to perform an action (e.g., tilt the device, draw a shapes, letters or patterns)
Cognitive	AccCAPTCHA [84]		2013	Play a simple rolling ball game or other well-known games (e.g., enigma, racing game)
	GISCHA [85]		2013	Play a simple game that consist of moving a ball to the destination hole with a specific shape
	SenCAPTCHA [95]		2020	Identify the animal eye position, then tilt the device to move the ball to this position.
	Ababtain et al. [86]		2019	Play a simple game that consist of one moving object (i.e., ball) and one or multiple target objects (e.g., Goal). Users move the device to match the ball with the target object.

TABLE VII: A taxonomy of sensor-based CAPTCHAs

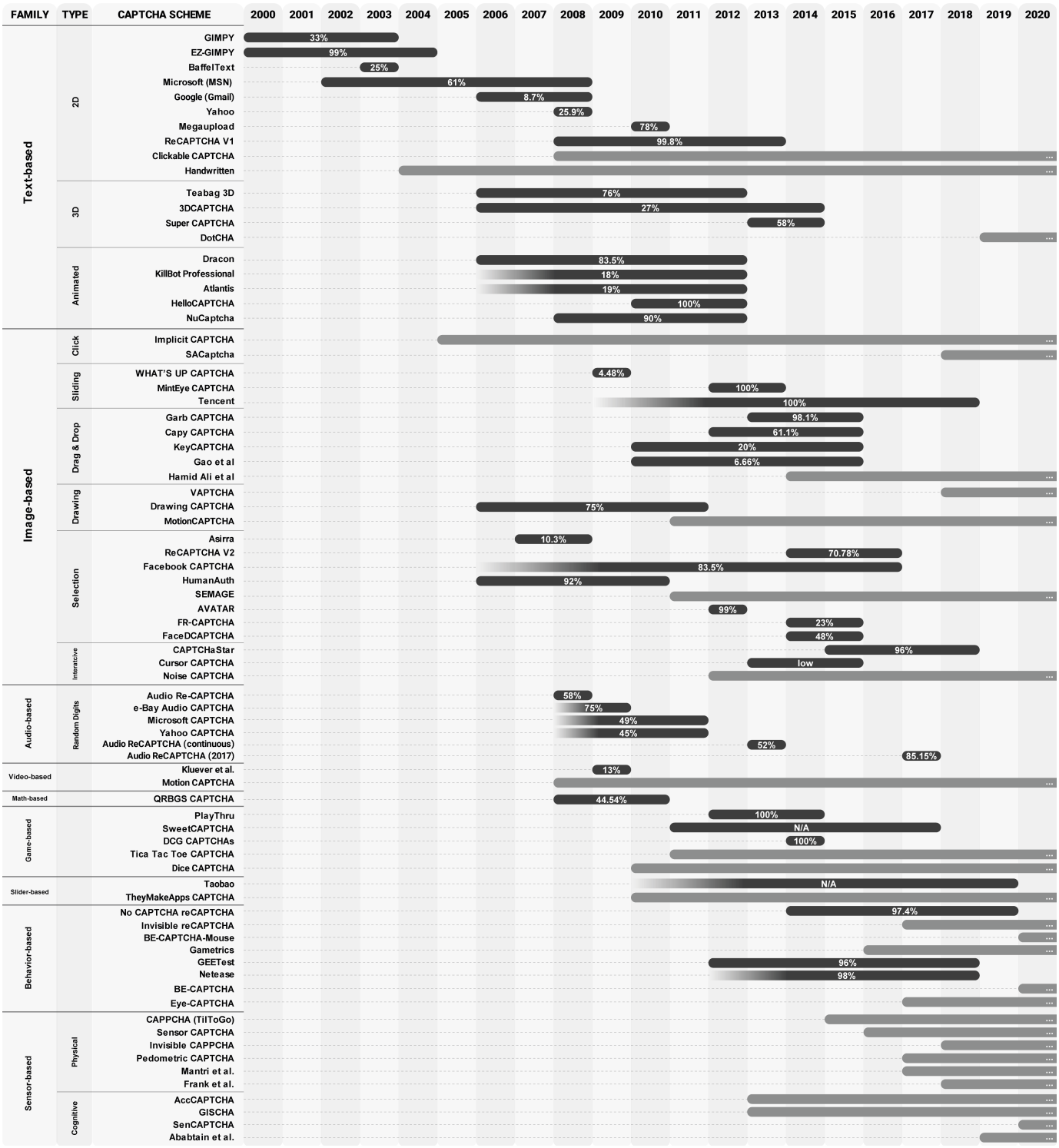


Fig. 1: Timeline of the security breaking of the CAPTCHA schemes

from Google [8] broke the hardest category of ReCAPTCHA using neural networks with an accuracy of 99.8%.

In [31], the authors discovered a set of attacks against 3D CAPTCHAs, even without the usage of OCR programs. In details, they were able to successfully extract a set of pixels from the characters of several 3D CAPTCHA schemes (i.e., Teabag 3D, 3dcaptcha, and Super CAPTCHA) that can be used for automated recognition of the challenge. Thanks to such a technique, the authors were able to achieve success rates of 31%, 58%, and 27% in breaking Teabag 3D, 3dcaptcha, and Super CAPTCHA, respectively. Furthermore, the same authors in [104] were able to break Teabag 3D with a higher success rate (i.e., 76%) by exploiting the side surface information contained in the 3D text objects.

Nguyen et al. [35] showed that the information across multiple animation frames in animated CAPTCHA schemes could be easily extracted using simple techniques such as the PDM (Pixel Delay Map) or CL (Catching Line) methods. They used these methods to defeat several animated CAPTCHAs with a high success rate, including iCAPTCHA, Atlantis, KillBot Professional, and Dracon CAPTCHA. In [97], the same methods have been used to defeat different types of HelloCAPTCHA schemes with a success rate between 16% - 100%, due to their weakness against segmentation attacks. Unlike HelloCAPTCHA, NuCaptcha is an animated CAPTCHA designed to be segmentation resistant. Since the characters are overlapped and crowded together, the PDM or CL methods used to defeat HelloCAPTCHA are not effective to separate the characters. However, NuCaptcha has been broken using more sophisticated attacks [105], [106]. Elie Bursztein [106] achieved a success rate of 90% by using bounding box shape analysis and an interest points (SIFT algorithm) density evaluation to isolate objects in each frame. Then he tracked these objects across multiple frames and kept only the 50 frames that contain the CAPTCHA answer.

B. Attacks against image-based CAPTCHA

Many attacks have been suggested in the literature to bypass the different type of image-based CAPTCHAs. Golle [107] was able to break the Asirra scheme with a success rate of 10.3%. To do so, he used different features to train an SVM (Support Vector Machine) classifier to identify cats and dogs with 82.7% accuracy (i.e., accuracy for a single image). Hernandez-Castro et al. in [13] proposed a side-channel attack that bypassed the HumanAuth challenge with a 92% success rate. Sivakorn et al. [10] have successfully attacked both Google and Facebook image-based CAPTCHA with success rates of 70.78% and 83.5%, respectively. In [75], the authors broke the new and the old variation of reCAPTCHA V2 with 79% and 88% success rates, respectively. Furthermore, they broke the Facebook image CAPTCHA and the China Railway CAPTCHA with success rates of 86% and 90%, respectively. Cheung [108] successfully broke Avatar CAPTCHA using Convolutional Neural Networks (CNN), with a high success rate of 99%. Gao et al. [109] broke both FR-CAPTCHA and FaceDCAPTCHA with success rates of 23% and 48%, respectively.

The Minteye CAPTCHA scheme was broken in [110], by exploiting the concept of Sobel operators and the length of the edges of the image. The idea behind this attack is based on the observation that the more an image is swirled, the longer the edges in the image become. So, the breaking methods consists in summing the length of the edges in the image and then select the image with the lowest sum of edges as the correct answer.

In [75], the authors broke different schemes of image-based CAPTCHAs, including the Tencent CAPTCHA. In detail, their proposal achieved 100% success rate even during the motion of the sliding puzzle to the target region. Hernandez-Castro et al. [12] proposed a very low-cost attack that does not attempt to solve image recognition or shape recognition problems but instead uses JPEG to measure the continuity of the image. Through this side-channel attack, they were able to bypass the most popular sliding-based CAPTCHAs. In detail, they break Capy CAPTCHA with a 65.1% success rate, and by applying minor modifications, they were able to break KeyCAPTCHA and Garb CAPTCHA as well with success rates of 20% and 98.1%, respectively. Conti el al [64] pointed out that Jigsaw CAPTCHA proposed by Gao et al. [50] is vulnerable to relay attack and random guess attack with a success rate of 6.66%. Lin et al. [111] broke Drawing CAPTCHA with an accuracy of 75%. They proposed an effective erosion-based breaking algorithm based on their observation of the difference between the size of the diamond-shaped dots and the dots used in the background as noise.

Although CAPTCHaStar authors tested its resiliency against several types of automated attacks such as traditional attacks, automated attacks using ad-hoc heuristics, and attacks based on machine learning, recently, Gougeon and Lacharme [112] were able to break this CAPTCHA with a 96% success rate. In addition, they pointed out that the modification of the parameters does not prevent CAPTCHaStar against their proposed attack, which is based on the concentration of pixels (i.e., stars) during the formation of the image. In [64] the authors pointed out that the resiliency of Cursor CAPTCHA to machine learning-based attacks and stream relay attack is low.

C. Attacks against audio-based CAPTCHA

Tam et al. [113] were the first to evaluate the robustness of audio CAPTCHAs against automated attacks. They were able to break audio reCAPTCHA using an SVM-based approach. They achieved a success rate of 45% when they matched the solution exactly and 58% when they leveraged a “one mistake” passing condition. Burzstein and Bethard [114] introduced Decaptcha, a system that was able to bypass the eBay’s audio CAPTCHAs with a 75% success rate. Their system applies a Discrete Fourier Transform (DFT) to the wave file and then isolates the energy spikes. Afterward, it uses a supervised learning algorithm to recognize speech patterns. In [115] the authors proposed a CAPTCHA solver based on the non-continuous speech, which defeated the Microsoft and the Yahoo audio CAPTCHAs with a success rate of 49% and 45%, respectively. The segmentation phase was unsupervised, while the classification phase was supervised. They used the Regularized Least-Squares Classification (RLSC) algorithm for classification, and Amazon Mechanical Turk to label scraped CAPTCHAs. However, their system was able to solve reCAPTCHA with only 1.5% success rate, due to the presence of semantic vocal noise. Sano et al. [116] developed a CAPTCHA solver for continuous CAPTCHAs that use overlapping target voices as defensive techniques to make automated segmentation difficult. Their system applied Hidden Markov Models (HMMs) for speech recognition. It was tested on the version of audio reCAPTCHA used in 2013, and the results show that it was able to break this version of continuous reCAPTCHA with a success rate of 52%. Bock et al. [117] introduced unCaptcha, an automated

system that can bypass audio reCAPTCHA released in 2017 with an 85.15% success rate. They attained these results by leveraging free online speech-to-text services and performing a minimal phonetic mapping to enhance accuracy.

D. *Attacks against Behavior-based CAPTCHA*

Although Sliding-based behavioral CAPTCHA schemes attempted to increase the security of sliding CAPTCHAs by detecting malicious behaviors, recently, Zhao et al. [75] were able to bypass such a detection by leveraging four simulation functions (i.e., Sigmoid, Softmax, ReLu, and Tanh) to mimic human behaviors. Their proposed attack against the GeeTest and Netease CAPTCHA schemes achieves the best success rate of 96% and 98% respectively, by using the Sigmoid function. Furthermore, Sivakorn et al. [10] found that Google's tracking cookies can be used to influence the risk analysis and, thus, bypass the reCAPTCHA V2 restrictions. In detail, the authors designed a tracking cookie for bots that was able, after nine days of automated browsing across different Google services, to fool the Google risk analysis system into thinking that the traffic is made by human beings and, consequently, to check the "I'm not a robot" box. Furthermore, the authors proposed a low-cost attack that breaks the second layer of reCAPTCHA V2 with a success rate of 70.78%. In [118], the authors used a "divide and conquer" strategy to defeat the No CAPTCHA reCAPTCHA scheme for any grid resolution. They achieved a success rate of 97.4% on a 100 x 100 grid and 96.7% on a 1000 x 1000 screen resolution.

E. *Attacks against the other type of CAPTCHA*

Kluever el al. [66] performed a tag frequency-based attack to evaluate the security of their proposed video-based CAPTCHA and achieved a success rate of 13%. Hernandez-Castro el al. [68] were able to break QRBGS CAPTCHA using a side-channel attack with a success rate of 44.54%. In [71], Mohamed et al. reported that DCG CAPTCHAs, including PlayThru, are vulnerable to dictionary-based automated attacks. In [119], a developer proposed a solver that automatically bypasses SweetCAPTCHA. In [120], different variations of slider CAPTCHAs, including the Taobao scheme, have been bypassed by using a simple JavaScript code and puppeteer.

IV. Evolution of CAPTCHA Schemes

The evolution of CAPTCHA schemes follows the advancements of technology to break them. In the early 2000s, text-based CAPTCHAs were the dominant solutions to discern between human and automated users. To this aim, security experts developed a set of attacks to break the most popular text-based schemes by leveraging image processing, pattern recognition, and machine learning algorithms [121]. Furthermore, the scientific community attempted to enhance the security of existing text-based CAPTCHAs by applying anti-segmentation and anti-recognition techniques. However, these countermeasures made text-based CAPTCHAs challenging even for human users, resulting in a higher error rate and limited usability that reduces text-based schemes' popularity. Finally, in 2014 a research conducted by Google demonstrated that the advancements in the AI technology could solve the most complicated variants of distorted text at 99.8% accuracy [8], leading to the decline of the text-based CAPTCHA schemes.

The security weaknesses of text-based CAPTCHAs and its usability issues, especially with the advent of mobile devices, led many researchers to look for alternatives. Since 2004, many of them have focused on exploiting Computer Vision (CV) problems such as image classification and object recognition that were considered harder AI problems than character recognition at that time. Chew and Tygar [122] were among the first researchers using labeled images to design image-based CAPTCHAs. After that, many images-based CAPTCHAs schemes have been proposed to create challenges that require selection, drag and drop or sliding of images to discern between human and automated usages. However, the advancement in CV and machine learning and the advent of Machine Learning as a service (MLaaS) solutions boosted the breaking of the major image-based CAPTCHA schemes between 2013 and 2018. For instance, the authors of [75] exploited ML to perform attacks against several image-based CAPTCHAs, including the image-based reCAPTCHA V2 scheme.

In conjunction with the advent of text-based and image-based CAPTCHAS, the security experts proposed Audio-based CAPTCHAs to cope with visually impaired users. However, those schemes are limited by language barriers and low usability, as discussed in [123]. Furthermore, they are also weak against supervised learning, and automatic Speech Recognition (ASR) attacks [124].

Starting from the 2010s, the research community introduced behavioral-based CAPTCHA schemes to build challenges based on behavioral biometrics measurements. The first deployed behavioral-based CAPTCHA was introduced in 2012 by the Geetest company, while in 2014, Google released No CAPTCHA reCAPTCHA and later on Invisible CAPTCHA (2017). Still, most of the commercial and academic proposals are based on mouse dynamics, which have been shown to be vulnerable to bots attacks that attempt to mimic the user's behavioral pattern [75], [1]. As shown in the timeline of Figure. 1, the most widespread behavioral CAPTCHAs (i.e., No CAPTCHA reCAPTCHA, GEETest, and Netease) have been broken with a high success rate [118], [75] in the last years.

In addition, behavioral-based CAPTCHA schemes raise serious privacy concerns as described in [125], [126], and [79]. For instance, [126] demonstrated how demographic attributes such as gender, age group, and education level could be extracted while solving a simple game CAPTCHA (e.g., Gametrics) by capturing user's innate cognitive abilities and behavioral patterns. Due to such concerns, Cloudflare recently decided to move away from reCAPTCHA [127].

Finally, the latest research directions exploit the data gathered from sensors to build challenges that are difficult to be emulated by automated bots. At the time of writing, no study has been done to review or analyze the security strength of

sensor-based CAPTCHAs, and none of the proposed solutions has been successfully bypassed.

V. Open Issues, Challenges and opportunities

In this section, we identify the open issues in designing robust and usable CAPTCHA schemes, as well as the main challenges that a CAPTCHA designer might have to deal with, and opportunities for further study.

A. Resilience to both automated and human solver relay attacks

A CAPTCHA scheme can be considered highly secure when both the automated attack success rate is less than 0.01% [27], [128] and it is resilient to human solver relay attacks. Unfortunately, in the literature most studies dedicated to the design of CAPTCHA schemes focus only on automated attacks while only few of them take into account the resilience to human solver relay attacks.

The security level of traditional CAPTCHA schemes depends on the hardness of some AI problem. However, the progress of AI techniques and computing power has led to the breaking of these CAPTCHA schemes with high success rates [8], [10], [75], [117]. Therefore, in order to design the next generation CAPTCHA schemes, it is important to move away from schemes based on hard AI problems toward other approaches less vulnerable to learning-based attacks [129]. Recently, big companies like Google, Alibaba and Tencent have migrated towards behavior-based CAPTCHA schemes, while there is an initiative aiming at deploying a sensor-based CAPTCHA scheme that uses the same key concept of Invisible CAPPCHA [83] by a company called Brave [126].

As presented in detail in Section 3, all the popular conventional CAPTCHA schemes have been broken with high success rate by automated attacks and most of them are also vulnerable to human solver relay attacks (the most notable exceptions being CAPTCHaStar, PlayThru and Dynamic Cognitive Game CAPTCHA). Similarly, popular behavior-based CAPTCHA schemes have also been broken with high success rate by automated attacks, and all of them are vulnerable to human solver attacks. Invisible reCAPTCHA and other academic proposals have not been broken yet, however with the advent of the fourth generation bots which rotate through thousands of different IP addresses and mimic accurately the human behavior, it would be difficult to design a secure CAPTCHA based solely on the user behavior data that can be gathered in a normal (i.e., with no additional sensors or special hardware) environment. None of the sensor-based CAPTCHA has been broken yet by automated attacks, however similar to the other types of CAPTCHA schemes, most of them are vulnerable to human solver relay attacks. The exception to this vulnerability is represented by the ones that have been specifically designed to resist this kind of attack (e.g., Invisible CAPPCHA). Another weakness of sensor-based CAPTCHA schemes is the limited number of challenges. This is due to the fact that designing a large number of usable gestures for instance, to ensure high security against automated attacks, is very challenging. However, this weakness may be solved relying on trusted hardware.

On the basis of the above observations, we identified the following open problems that require further study in order to design robust and usable CAPTCHA schemes: it is necessary to investigate 1) the resilience of currently unbroken behavior-based CAPTCHAs against fourth generation bots; 2) the security strength of sensor-based CAPTCHA schemes against replay attacks, sensor manipulation [130] and human solver relay attacks 3) the security of CAPTCHA schemes that make validation process at the client-side either with or without secure hardware as they may be hacked.

B. Friction-heavy vs. Frictionless Challenges

CAPTCHA schemes are well known as a source of annoyance to users. This is due to the fact that most of the time designers trying to make the scheme more secure also make the challenge harder for humans. It is important to reduce the friction in general and the cognitive overload associated to the challenges. Creating user-friendly CAPTCHAs, yet, it is not always an easy task and in many cases there is a trade-off between security and usability. Some CAPTCHA schemes achieve complete transparency to users (i.e., invisible reCAPTCHA, invisible CAPPCHA) removing all cognitive challenges. However, it is worth noting that not all the CAPTCHA schemes in the same category (i.e., behavioral-based and sensor-based) are automatically endowed with the same level of usability. In fact, while some of them require a simple task such as clicking on a check box or tilting the device, others requires less user-friendly tasks such as solving a complex cognitive task, performing a physical task such as walking few steps or performing complex gestures.

To the best of our knowledge, there is no study fully dedicated to the analysis of the usability of behavior-based and sensor-based CAPTCHA schemes. Therefore, we argue that such a study would allow assessing the level of usability of all the CAPTCHA schemes proposed in the behavioral-based and sensor-based categories.

C. Preserving the user's privacy

Unlike traditional CAPTCHA schemes, it has been shown that the new behavior-based and sensor-based CAPTCHA schemes may raise a privacy issue when information such as user's behavioral data, sensor data and cookies that can be used for tracking are sent to a remote server. As a solution, some researchers suggested to send solely the results of the test to the server, instead of the sensor data. However, trusted hardware is then required to prevent hacking at the client side. Further study is needed to identify methodologies capable of preventing client-side hacking without requiring trusted hardware. Besides, the user's privacy should be taken into strong consideration in general from the very start of the design phase of new CAPTCHA schemes.

D. Compatibility with all devices

A robust and usable CAPTCHA scheme that is compatible with different form factors is obviously highly desirable,

however, the most promising CAPTCHA schemes category in term of security and usability present a significant dependency on a specific form factor. For instance, behavioral-based CAPTCHA schemes strongly rely on mouse dynamics or on touch-and-tap dynamics, hence they require form-factor specialization. Sensor-based CAPTCHA schemes require sensors that are available only in tablets, smartphones and smartwatches (e.g., [91], [94]), hence they are currently unavailable on a large portion of users' devices and further study to find potential surrogates of sensors data, possibly relying on trusted hardware, on desktops and laptops are needed.

VI. Conclusion

CAPTCHA has been widely used as a security mechanism to prevent bots from abusing online services. Over the years, different types of CAPTCHA schemes have been proposed, mainly to improve the usability and the security against new threats presented by evolving bots. The studies in the literature usually focus on the conventional CAPTCHA schemes, i.e., text, image and audio based schemes, and do not take into account either new types of schemes or novel threats such as human solver relay attacks, sensor manipulation [130] and the risk of privacy breaches. In this paper, we have provided a comprehensive review of the related research involving two decades, by also highlighting the new trends and open issues. We have first presented a comprehensive classification of the current CAPTCHA schemes that includes both traditional and new ones. Then, to evaluate their drawbacks from the security point of view, we have provided a detailed summary on the attack methods that have been used to break CAPTCHA schemes in each category. Finally, we have discussed the current state-of-the-art in the field of CAPTCHA schemes design, highlighting the open issues, the challenges, and the opportunities for further research that constitute the road toward the design of the next generation of secure and user-friendly CAPTCHA schemes.

References

[1] Radware. (2020) The big bad bot problem 2020.
[2] M. Guerar, B. Mohamed, and V. Alimi, "Color wheel pin: Usable and resilient atm authentication," *Journal of High Speed Networks*, vol. 22, pp. 231–240, 06 2016.
[3] S. Rees-Pullman, "Is credential stuffing the new phishing?" *Computer Fraud & Security*, vol. 2020, no. 7, pp. 16 – 19, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1361372320300762
[4] M. Naor, "Verification of a human in the loop or identification via the turing test," 1996.
[5] M. Lillibridge, M. Abadi, K. Bharat, and A. Broder, "Method for selectively restricting access to computer systems," Patent 6 195 698, February, 2001. [Online]. Available: http://www.freepatentsonline.com/6195698.html
[6] L. von Ahn, M. Blum, N. Hopper, and J. Langford. (2000) Captcha: Telling humans and computers apart automatically. [Online]. Available: http://www.captcha.net/
[7] L. Von Ahn, M. Blum, N. J. Hopper, and J. Langford, "Captcha: Using hard ai problems for security," in *International conference on the theory and applications of cryptographic techniques*. Springer, 2003, pp. 294–311.
[8] I. J. Goodfellow, Y. Bulatov, J. Ibarz, S. Arnoud, and V. D. Shet, "Multi-digit number recognition from street view imagery using deep convolutional neural networks," *CoRR*, vol. abs/1312.6082, 2014.
[9] K. Chellapilla and P. Y. Simard, "Using machine learning to break visual human interaction proofs (hips)," in *Proceedings of the 17th International Conference on Neural Information Processing Systems*, ser. NIPS'04. Cambridge, MA, USA: MIT Press, 2004, p. 265–272. [Online]. Available: https://doi.org/10.5555/2976040.2976074
[10] S. Sivakorn, J. Polakis, and A. D. Keromytis, "I'm not a human : Breaking the google recaptcha," in *BlackHat 2016*, 2016.
[11] C. Fritsch, M. Netter, A. Reisser, and G. Pernul, "Attacking image recognition captchas," in *Trust, Privacy and Security in Digital Business*, S. Katsikas, J. Lopez, and M. Soriano, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 13–25. [Online]. Available: https://doi.org/10.1007/978-3-642-35130-3_23
[12] C. J. Hernández-Castro, M. D. R-Moreno, and D. F. Barrero, "Using jpeg to measure image continuity and break capy and other puzzle captchas," *IEEE Internet Computing*, vol. 19, no. 6, pp. 46–53, 2015. [Online]. Available: https://doi.org/10.1109/MIC.2015.127
[13] C. J. Hernandez-Castro, A. Ribagorda, and Y. Saez, "Side-channel attack on the humanauth captcha," in *2010 International Conference on Security and Cryptography (SECRYPT)*, 2010, pp. 1–7.
[14] V. Shet. (2014) Are you a robot? introducing "no captcha recaptcha". [Online]. Available: https://security.googleblog.com/2014/12/are-you-robot-introducing-no-captcha.html
[15] Y. Zi, H. Gao, Z. Cheng, and Y. Liu, "An end-to-end attack on text captchas," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 753–766, 2020. [Online]. Available: https://doi.org/10.1109/TIFS.2019.2928622
[16] P. Wang, H. Gao, Z. Shi, Z. Yuan, and J. Hu, "Simple and easy: Transfer learning-based attacks to text captcha," *IEEE Access*, vol. 8, pp. 59 044–59 058, 2020. [Online]. Available: https://doi.org/10.1109/ACCESS.2020.2982945
[17] D. D. Ferreira, L. Leira, P. Mihaylova, and P. Georgieva, "Breaking text-based captcha with sparse convolutional neural networks," in *Pattern Recognition and Image Analysis*, A. Morales, J. Fierrez, J. S. Sánchez, and B. Ribeiro, Eds. Cham: Springer International Publishing, 2019, pp. 404–415. [Online]. Available: https://doi.org/10.1007/978-3-030-31321-0_35
[18] D. Brodić and A. Amelio, "Exploring the usability of the text-based captcha on tablet computers," *Connection Science*, vol. 31, no. 4, pp. 430–444, 2019. [Online]. Available: https://doi.org/10.1080/09540091.2019.1609417
[19] X. Xu, L. Liu, and B. Li, "A survey of captcha technologies to distinguish between human and computer," *Neurocomputing*, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0925231220304896
[20] Y. Zhang, H. Gao, G. Pei, S. Luo, G. Chang, and N. Cheng, "A survey of research on captcha designing and breaking techniques," in *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2019, pp. 75–84. [Online]. Available: https://doi.org/10.1109/TrustCom/BigDataSE.2019.00020
[21] Y.-W. Chow, W. Susilo, and P. Thorncharoensri, *CAPTCHA Design and Security Issues*. Singapore: Springer Singapore, 2019, pp. 69–92. [Online]. Available: https://doi.org/10.1007/978-981-13-1483-4_4
[22] D. Brodić and A. Amelio, *Types of CAPTCHA*. Cham: Springer International Publishing, 2020, pp. 29–32. [Online]. Available: https://doi.org/10.1007/978-3-030-29345-1_6
[23] V. P. Singh and P. Pal, "Survey of different types of captcha," *International Journal of Computer Science and Information Technologies*, vol. 5, no. 2, pp. 2242–2245, 2014.
[24] L. von Ahn; Manuel Blum; Nick Hopper; John Langford; Udi Manber. (2000) Gimpy. [Online]. Available: http://www.captcha.net/captchas/gimpy/
[25] M. Chew and H. S. Baird, "BaffleText: a human interactive proof," in *Document Recognition and Retrieval X*, T. Kanungo, E. H. B. Smith, J. Hu, and P. B. Kantor, Eds., vol. 5010, International Society for Optics and Photonics. SPIE, 2003, pp. 305 – 316. [Online]. Available: https://doi.org/10.1117/12.479682
[26] L. von Ahn, B. Maurer, C. McMillen, D. Abraham, and M. Blum, "recaptcha: Human-based character recognition via web security measures," *Science*, vol. 321, no. 5895, pp. 1465–1468, 2008. [Online]. Available: http://www.sciencemag.org/content/321/5895/1465.full.pdf
[27] J. Yan and A. S. El Ahmad, "A low-cost attack on a microsoft captcha," in *Proceedings of the 15th ACM Conference on Computer and Communications Security*, ser. CCS '08. New York, NY, USA: Association for Computing Machinery, 2008, p. 543–554. [Online]. Available: https://doi.org/10.1145/1455770.1455839

[28] R. Chow, P. Golle, M. Jakobsson, L. Wang, and X. Wang, "Making captchas clickable," in *Proceedings of the 9th Workshop on Mobile Computing Systems and Applications*, ser. HotMobile '08. New York, NY, USA: Association for Computing Machinery, 2008, p. 91–94. [Online]. Available: https://doi.org/10.1145/1411759.1411783

[29] A. Rusu and V. Govindaraju, "Handwritten captcha: using the difference in the abilities of humans and machines in reading handwritten words," in *Ninth International Workshop on Frontiers in Handwriting Recognition*, 2004, pp. 226–231. [Online]. Available: https://doi.org/10.1109/IWFHR.2004.54

[30] (2006) Ocr research team, teabag 3d evolution. [Online]. Available: https://ocr-research.org.ua/teabag.html

[31] V. D. Nguyen, Y.-W. Chow, and W. Susilo, "On the security of text-based 3d captchas," *Computers & Security*, vol. 45, pp. 84 – 99, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404814000856

[32] M. L. Wells. (2003) Exciting features in super captcha. [Online]. Available: https://goldsborowebdevelopment.com/2013/06/exciting-features-in-super-captcha/

[33] S. Kim and S. Choi, "Dotcha: A 3d text-based scatter-type captcha," in *Web Engineering*, M. Bakaev, F. Frasincar, and I.-Y. Ko, Eds. Cham: Springer International Publishing, 2019, pp. 238–252. [Online]. Available: https://doi.org/10.1007/978-3-030-19274-7_18

[34] (2006) Dracon visual flash captcha. [Online]. Available: https://www.dracon.biz/captcha.php

[35] V. D. Nguyen, Y.-W. Chow, and W. Susilo, "Attacking animated captchas via character extraction," in *Cryptology and Network Security*, J. Pieprzyk, A.-R. Sadeghi, and M. Manulis, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 98–113. [Online]. Available: https://doi.org/10.1007/978-3-642-35404-5_9

[36] *Program Product, HelloCAPTCHA*. [Online]. Available: http://www.hellocaptcha.com/

[37] Nucaptcha inc, nucaptcha. [Online]. Available: https://www.nucaptcha.com

[38] A. Rusu and V. Govindaraju, "Visual captcha with handwritten image analysis," in *Human Interactive Proofs*, H. S. Baird and D. P. Lopresti, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 42–52. [Online]. Available: https://doi.org/10.1007/11427896_3

[39] M. Imsamai and S. Phimoltares, "3d captcha: A next generation of the captcha," in *2010 International Conference on Information Science and Applications*, 2010, pp. 1–8. [Online]. Available: https://doi.org/10.1109/ICISA.2010.5480258

[40] I. Fischer and T. Herfet, "Visual captchas for document authentication," in *2006 IEEE Workshop on Multimedia Signal Processing*, 2006, pp. 471–474. [Online]. Available: https://doi.org/10.1109/MMSP.2006.285353

[41] A. B. Naumann, T. Franke, and C. Bauckhage, "Investigating captchas based on visual phenomena," in *Human-Computer Interaction – INTERACT 2009*, T. Gross, J. Gulliksen, P. Kotzé, L. Oestreicher, P. Palanque, R. O. Prates, and M. Winckler, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 745–748. [Online]. Available: https://doi.org/10.1007/978-3-642-03658-3_79

[42] J. Cui, J. Mei, X. Wang, D. Zhang, and W. Zhang, "A captcha implementation based on 3d animation," in *2009 International Conference on Multimedia Information Networking and Security*, vol. 2, 2009, pp. 179–182. [Online]. Available: https://doi.org/10.1109/MINES.2009.298

[43] H. S. Baird and J. L. Bentley, "Implicit CAPTCHAs," in *Document Recognition and Retrieval XII*, E. H. B. Smith and K. Taghva, Eds., vol. 5676, International Society for Optics and Photonics. SPIE, 2005, pp. 191 – 196. [Online]. Available: https://doi.org/10.1117/12.590944

[44] M. Tang, H. Gao, Y. Zhang, Y. Liu, P. Zhang, and P. Wang, "Research on deep learning techniques in breaking text-based captchas and designing image-based captcha," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 10, pp. 2522–2537, 2018. [Online]. Available: https://doi.org/10.1109/TIFS.2018.2821096

[45] R. Gossweiler, M. Kamvar, and S. Baluja, "What's up captcha? a captcha based on image orientation," in *Proceedings of the 18th International Conference on World Wide Web*, ser. WWW '09. New York, NY, USA: Association for Computing Machinery, 2009, p. 841–850. [Online]. Available: https://doi.org/10.1145/1526709.1526822

[46] (2012) Blog post, minteye offers no-type captcha as a security twist. [Online]. Available: https://phys.org/news/2012-12-minteye-no-type-captcha.html

[47] Garb captcha. [Online]. Available: https://me.wordpress.org/plugins/captcha-garb/

[48] Capy inc, capy puzzle captcha. [Online]. Available: https://www.capy.me/products/puzzle_captcha/

[49] Keycaptcha. [Online]. Available: https://www.keycaptcha.com/

[50] H. Gao, D. Yao, H. Liu, X. Liu, and L. Wang, "A novel image based captcha using jigsaw puzzle," in *2010 13th IEEE International Conference on Computational Science and Engineering*, 2010, pp. 351–356. [Online]. Available: https://doi.org/10.1109/CSE.2010.53

[51] F. A. B. Hamid Ali and F. B. Karim, "Development of captcha system based on puzzle," in *2014 International Conference on Computer, Communications, and Control Technology (I4CT)*, 2014, pp. 426–428. [Online]. Available: https://doi.org/10.1109/I4CT.2014.6914219

[52] J. Elson, J. R. Douceur, J. Howell, and J. Saul, "Asirra: A captcha that exploits interest-aligned manual image categorization," in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, ser. CCS '07. New York, NY, USA: Association for Computing Machinery, 2007, pp. 366–374. [Online]. Available: https://doi.org/10.1145/1315245.1315291

[53] Neo. (2006) Blog post, [humanauth] verification code for natural patterns. [Online]. Available: http://www.neo.com.tw/archives/965

[54] S. Vikram, Y. Fan, and G. Gu, "Semage: A new image-based two-factor captcha," in *Proceedings of the 27th Annual Computer Security Applications Conference*, ser. ACSAC '11. New York, NY, USA: Association for Computing Machinery, 2011, p. 237–246. [Online]. Available: https://doi.org/10.1145/2076732.2076766

[55] D. D'Souza, P. C. Polina, and R. V. Yampolskiy, "Avatar captcha: Telling computers and humans apart via face classification," in *2012 IEEE International Conference on Electro/Information Technology*, 2012, pp. 1–6. [Online]. Available: https://doi.org/10.1109/EIT.2012.6220734

[56] G. Goswami, B. M. Powell, M. Vatsa, R. Singh, and A. Noore, "Fr-captcha: Captcha based on recognizing human faces," *PLoS ONE*, vol. 9, 2014. [Online]. Available: https://doi.org/10.1371/journal.pone.0091708

[57] G. Goswami, B. Powell, M. Vatsa, R. Singh, and A. Noore, "Facedcaptcha: Face detection based color image captcha," *Future Generation Computer Systems*, vol. 31, pp. 59–68, 2014. [Online]. Available: https://doi.org/10.1016/j.future.2012.08.013

[58] C. Yuan, Jingxia (Chongqing, "Variation analysis-based public turing test to tell computers and humans apart," Patent 20 180 253 542, September, 2018. [Online]. Available: http://www.freepatentsonline.com/y2018/0253542.html

[59] M. Shirali-Shahreza and S. Shirali-Shahreza, "Drawing captcha," in *28th International Conference on Information Technology Interfaces, 2006.*, 2006, pp. 475–480. [Online]. Available: https://doi.org/10.1109/ITI.2006.1708527

[60] Motioncaptcha v0.2, stop spam, draw shapes. [Online]. Available: http://www.josscrowcroft.com/demos/motioncaptcha/

[61] V. A. Thomas and K. Kaur, "Cursor captcha — implementing captcha using mouse cursor," in *2013 Tenth International Conference on Wireless and Optical Communications Networks (WOCN)*, 2013, pp. 1–5. [Online]. Available: https://doi.org/10.1109/WOCN.2013.6616188

[62] M. Okada and S. Matsuyama, "New captcha for smartphones and tablet pc," in *2012 IEEE Consumer Communications and Networking Conference (CCNC)*, 2012, pp. 34–35. [Online]. Available: https://doi.org/10.1109/CCNC.2012.6181038

[63] Google. Choosing the type of recaptcha. [Online]. Available: https://developers.google.com/recaptcha/docs/versions

[64] M. Conti, C. Guarisco, and R. Spolaor, "Captchastar! a novel captcha based on interactive shape discovery," in *Applied Cryptography and Network Security*, M. Manulis, A.-R. Sadeghi, and S. Schneider, Eds. Cham: Springer International Publishing, 2016, pp. 611–628. [Online]. Available: https://doi.org/10.1007/978-3-319-39555-5_33

[65] G. Sauer, J. Holman, J. Lazar, H. Hochheiser, and J. Feng, "Accessible privacy and security: A universally usable human-interaction proof tool," *Univers. Access Inf. Soc.*, vol. 9, no. 3, p. 239–248, Aug. 2010. [Online]. Available: https://doi.org/10.1007/s10209-009-0171-2

[66] K. A. Kluever and R. Zanibbi, "Balancing usability and security in a video captcha," in *Proceedings of the 5th Symposium on Usable Privacy and Security*, ser. SOUPS '09. New York, NY, USA: Association for Computing Machinery, 2009. [Online]. Available: https://doi.org/10.1145/1572532.1572551

[67] M. Shirali-Shahreza and S. Shirali-Shahreza, "Motion captcha," in *2008 Conference on Human System Interactions*, 2008, pp. 1042–1044. [Online]. Available: https://doi.org/10.1109/HSI.2008.4581589

[68] C. J. Hernandez-Castro and A. Ribagorda, "Pitfalls in captcha design and implementation: The math captcha, a case study," *Computers &*

Security, vol. 29, no. 1, pp. 141 – 157, 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404809000728

[69] L. Wroblewski. (2010) A sliding alternative to captcha? [Online]. Available: https://www.lukew.com/ff/entry.asp?1138

[70] Are you a human inc, playthru: A captcha alternative from are you a human. [Online]. Available: https://developer.salesforce.com/index.php?title=PlayThru:_A_CAPTCHA_Alternative_from_Are_You_a_Human&oldid=50650

[71] M. Mohamed, N. Sachdeva, M. Georgescu, S. Gao, N. Saxena, C. Zhang, P. Kumaraguru, P. C. van Oorschot, and W.-B. Chen, "A three-way investigation of a game-captcha: Automated attacks, relay attacks and usability," in *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security*, ser. ASIA CCS '14. New York, NY, USA: Association for Computing Machinery, 2014, p. 195–206. [Online]. Available: https://doi.org/10.1145/2590296.2590298

[72] Dice captcha, 2010. [Online]. Available: http://dice-captcha.com/demo-dice-captcha.php

[73] A. Acien, A. Morales, J. Fiérrez, and R. Vera-Rodriguez, "Becaptcha-mouse: Synthetic mouse trajectories and improved bot detection," *ArXiv*, vol. abs/2005.00890, 2020.

[74] M. Mohamed and N. Saxena, "Gametrics: towards attack-resilient behavioral authentication with simple cognitive games," *Proceedings of the 32nd Annual Conference on Computer Security Applications*, 2016. [Online]. Available: https://doi.org/10.1145/2991079.2991096

[75] B. Zhao, H. Weng, S. Ji, J. Chen, T. Wang, Q. He, and R. Beyah, "Towards evaluating the security of real-world deployed image captchas," in *Proceedings of the 11th ACM Workshop on Artificial Intelligence and Security*, ser. AISec '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 85–96. [Online]. Available: https://doi.org/10.1145/3270101.3270104

[76] A. Acien, A. Morales, J. Fierrez, R. Vera-Rodriguez, and I. Bartolome, "Be-captcha: Detecting human behavior in smartphone interaction using multiple inbuilt sensors," in *AAAI Workshop on Artificial for Cyber Security (AICS)*, February 2020.

[77] A. Siripitakchai, S. Phimoltares, and A. Mahaweerawat, "Eye-captcha: An enhanced captcha using eye movement," in *2017 3rd IEEE International Conference on Computer and Communications (ICCC)*, 2017, pp. 2120–2126. [Online]. Available: https://doi.org/10.1109/CompComm.2017.8322911

[78] M. Guerar, M. Migliardi, A. Merlo, M. Benmohammed, and B. Messabih, "A completely automatic public physical test to tell computers and humans apart: A way to enhance authentication schemes in mobile devices," in *2015 International Conference on High Performance Computing Simulation (HPCS)*, July 2015, pp. 203–210.

[79] T. Hupperich, K. Krombholz, and T. Holz, "Sensor captchas: On the usability of instrumenting hardware sensors to prove liveliness," in *Trust and Trustworthy Computing*, M. Franz and P. Papadimitratos, Eds. Cham: Springer International Publishing, 2016, pp. 40–59. [Online]. Available: https://doi.org/10.1007/978-3-319-45572-3_3

[80] S. Kulkarni and H. S. Fadewar, "Pedometric captcha for mobile internet users," in *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT)*, 2017, pp. 600–604. [Online]. Available: https://doi.org/10.1109/RTEICT.2017.8256667

[81] V. C. Mantri and P. Mehrotra, "User authentication based on physical movement information," Patent 9 864 854, January, 2018. [Online]. Available: http://www.freepatentsonline.com/9864854.html

[82] B. Z. Frank and J. A. Latone, "Verifying a user utilizing gyroscopic movement," Patent 9 942 768, April, 2018. [Online]. Available: http://www.freepatentsonline.com/9942768.html

[83] M. Guerar, A. Merlo, M. Migliardi, and F. Palmieri, "Invisible cappcha: A usable mechanism to distinguish between malware and humans on the mobile iot," *Computers & Security*, vol. 78, pp. 255 – 266, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404818307557

[84] C.-J. Liao, C.-J. Yang, J.-T. Yang, H.-Y. Hsu, and J.-W. Liu, "A game and accelerometer-based captcha scheme for mobile learning system," in *Proceedings of EdMedia + Innovate Learning 2013*, J. Herrington, A. Couros, and V. Irvine, Eds. Victoria, Canada: Association for the Advancement of Computing in Education (AACE), June 2013, pp. 1385–1390. [Online]. Available: https://www.learntechlib.org/p/112139

[85] T.-I. Yang, C.-S. Koong, and C.-C. Tseng, "Game-based image semantic captcha on handset devices," *Multimedia Tools and Applications*, vol. 74, pp. 5141–5156, 2013. [Online]. Available: https://doi.org/10.1007/s11042-013-1666-7

[86] E. Ababtain and D. Engels, "Gestures based captchas the use of sensor readings to solve captcha challenge on smartphones," in *2019 International Conference on Computational Science and Computational Intelligence (CSCI)*, 2019, pp. 113–119. [Online]. Available: https://doi.org/10.1109/CSCI49370.2019.00026

[87] Imperva. (2020) 2020 bad bot report. [Online]. Available: https://www.imperva.com/resources/reports/Imperva_BadBot_Report_V2.0.pdf

[88] S. Popoveniuc, "Speakup: remote unsupervised voting," in *Industrial Track ACNS*, 2010.

[89] E. Uzun, S. P. H. Chung, I. Essa, and W. Lee, "rtcaptcha: A real-time captcha based liveness detection system," in *NDSS*, 2018. [Online]. Available: https://doi.org/10.14722/ndss.2018.23253

[90] M. Guerar, M. Migliardi, A. Merlo, M. Benmohammed, F. Palmieri, and A. Castiglione, "Using screen brightness to improve security in mobile social network access," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 621–632, 2018. [Online]. Available: https://doi.org/10.1109/TDSC.2016.2601603

[91] M. Guerar, M. Migliardi, F. Palmieri, L. Verderame, and A. Merlo, "Securing pin-based authentication in smartwatches with just two gestures," *Concurrency and Computation: Practice and Experience*, vol. 32, no. 18, p. e5549, 2020.

[92] M. Guerar, L. Verderame, M. Migliardi, and A. Merlo, "2gesturepin: Securing pin-based authentication on smartwatches," in *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, 2019, pp. 327–333. [Online]. Available: https://doi.org/10.1109/WETICE.2019.00074

[93] M. Guerar, A. Merlo, and M. Migliardi, "Completely automated public physical test to tell computers and humans apart: A usability study on mobile devices," *Future Generation Computer Systems*, vol. 82, pp. 617 – 630, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17303709

[94] M. Guerar, L. Verderame, A. Merlo, F. Palmieri, M. Migliardi, and L. Vallerini, "Circlepin: A novel authentication mechanism for smartwatches to prevent unauthorized access to iot devices," *ACM Trans. Cyber-Phys. Syst.*, vol. 4, no. 3, Mar. 2020. [Online]. Available: https://doi.org/10.1145/3365995

[95] Y. Feng, Q. Cao, H. Qi, and S. Ruoti, "Sencaptcha: A mobile-first captcha using orientation sensors," in *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 4, no. 2, 2020, pp. 1–26. [Online]. Available: https://doi.org/10.1145/3397312

[96] N. Roshanbin and J. Miller, "A survey and analysis of current captcha approaches," *J. Web Eng.*, vol. 12, no. 1–2, p. 1–40, Feb. 2013. [Online]. Available: https://doi.org/10.5555/2481562.2481563

[97] V. D. Nguyen, Y.-W. Chow, and W. Susilo, "Breaking an animated captcha scheme," in *Applied Cryptography and Network Security*, F. Bao, P. Samarati, and J. Zhou, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 12–29. [Online]. Available: https://doi.org/10.1007/978-3-642-31284-7_2

[98] G. Mori and J. Malik, "Recognizing objects in adversarial clutter: breaking a visual captcha," in *2003 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2003. Proceedings.*, vol. 1, 2003, pp. I–I. [Online]. Available: https://doi.org/10.1109/CVPR.2003.1211347

[99] G. Moy, N. Jones, C. Harkless, and R. Potter, "Distortion estimation techniques in solving visual captchas," in *Proceedings of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2004. CVPR 2004.*, vol. 2, 2004, pp. II–II. [Online]. Available: https://doi.org/10.1109/CVPR.2004.1315140

[100] K. Chellapilla, K. Larson, P. Simard, and M. Czerwinski, "Computers beat humans at single character recognition in reading based human interaction proofs (hips)," in *In 2nd Conference on Email and Anti-Spam*, 2005.

[101] K. Chellapilla, K. Larson, P. Y. Simard, and M. Czerwinski, "Building segmentation based human-friendly human interaction proofs (hips)," in *Human Interactive Proofs*, H. S. Baird and D. P. Lopresti, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 1–26. [Online]. Available: https://doi.org/10.1007/11427896_1

[102] J. "Yan and A. S. El Ahmad, "Is cheap labour behind the scene? - low-cost automated attacks on yahoo captchas," School of Computing Science, Newcastle University, England, Technical Report, 2008.

[103] A. S. El Ahmad, J. Yan, and L. Marshall, "The robustness of a new captcha," in *Proceedings of the Third European Workshop on System Security*, ser. EUROSEC '10. New York, NY, USA: Association for Computing Machinery, 2010, p. 36–41. [Online]. Available: https://doi.org/10.1145/1752046.1752052

[104] V. D. Nguyen, Y.-W. Chow, and W. Susilo, "Breaking a 3d-based captcha scheme," in *Information Security and Cryptology - ICISC 2011*, H. Kim, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 391–405. [Online]. Available: https://doi.org/10.1007/978-3-642-31912-9_26

[105] Y. Xu, G. Reynaga, S. Chiasson, J. Frahm, F. Monrose, and P. C. van Oorschot, "Security analysis and related usability of motion-based captchas: Decoding codewords in motion," *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 5, pp. 480–493, 2014. [Online]. Available: https://doi.org/10.1109/TDSC.2013.52

[106] E. Bursztein. (2012) How we broke the nucaptcha video scheme and what we propose to fix it. [Online]. Available: https://elie.net/blog/security/how-we-broke-the-nucaptcha-video-scheme-and-what-we-propose-to-fix-it/

[107] P. Golle, "Machine learning attacks against the asirra captcha," in *Proceedings of the 15th ACM Conference on Computer and Communications Security*, ser. CCS '08. New York, NY, USA: Association for Computing Machinery, 2008, p. 535–542. [Online]. Available: https://doi.org/10.1145/1455770.1455838

[108] B. Cheung, "Convolutional neural networks applied to human face classification," in *2012 11th International Conference on Machine Learning and Applications*, vol. 2, 2012, pp. 580–583. [Online]. Available: https://doi.org/10.1109/ICMLA.2012.177

[109] H. Gao, L. Lei, X. Zhou, J. Li, and X. Liu, "The robustness of face-based captchas," in *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, 2015, pp. 2248–2255. [Online]. Available: https://doi.org/10.1109/CIT/IUCC/DASC/PICOM.2015.332

[110] Jack. (2013) Breaking the minteye image captcha in 23 lines of python. [Online]. Available: http://www.jwandrews.co.uk/2013/01/breaking-the-minteye-image-captcha-in-23-lines-of-python/

[111] R. Lin, S.-Y. Huang, G. B. Bell, and Y.-K. Lee, "A new captcha interface design for mobile devices," in *Proceedings of the Twelfth Australasian User Interface Conference - Volume 117*, ser. AUIC '11. AUS: Australian Computer Society, Inc., 2011, p. 3–8.

[112] T. Gougeon and P. Lacharme, "How to break captchastar," in *ICISSP*, 2018. [Online]. Available: https://doi.org/10.5220/0006577600410051

[113] J. Tam, S. Hyde, J. Simsa, and L. V. Ahn, "Breaking audio captchas," in *Proceedings of the 21st International Conference on Neural Information Processing Systems*, ser. NIPS'08. Red Hook, NY, USA: Curran Associates Inc., 2008, p. 1625–1632.

[114] E. Bursztein and S. Bethard, "Decaptcha: breaking 75% of ebay audio captchas," in *Proceedings of the 3rd USENIX conference on Offensive technologies*, vol. 1, no. 8. USENIX Association, 2009, p. 8.

[115] E. Bursztein, R. Beauxis, H. Paskov, D. Perito, C. Fabry, and J. Mitchell, "The failure of noise-based non-continuous audio captchas," in *2011 IEEE Symposium on Security and Privacy*, 2011, pp. 19–31. [Online]. Available: https://doi.org/10.1109/SP.2011.14

[116] S. Sano, T. Otsuka, and H. G. Okuno, "Solving google's continuous audio captcha with hmm-based automatic speech recognition," in *Advances in Information and Computer Security*, K. Sakiyama and M. Terada, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 36–52. [Online]. Available: https://doi.org/10.1007/978-3-642-41383-4_3

[117] K. Bock, D. Patel, G. Hughey, and D. Levin, "Uncaptcha: A low-resource defeat of recaptcha's audio challenge," in *Proceedings of the 11th USENIX Conference on Offensive Technologies*, ser. WOOT'17. USA: USENIX Association, 2017, p. 7.

[118] I. Akrout, A. Feriani, and M. Akrout, "Hacking google recaptcha v3 using reinforcement learning," *ArXiv*, vol. abs/1903.01003, 2019.

[119] Sweet captcha solver. [Online]. Available: https://github.com/drdre1/Adultddl-Sweet-Captcha-Solver

[120] F. Vitas. (2019) How to bypass "slider captcha" with js and puppeteer. [Online]. Available: https://medium.com/@filipvitas/how-to-bypass-slider-captcha-with-js-and-puppeteer-cd5e28105e3c

[121] E. Bursztein, M. Martin, and J. Mitchell, "Text-based captcha strengths and weaknesses," in *Proceedings of the 18th ACM Conference on Computer and Communications Security*, ser. CCS '11. New York, NY, USA: Association for Computing Machinery, 2011, p. 125–138. [Online]. Available: https://doi.org/10.1145/2046707.2046724

[122] M. Chew and J. D. Tygar, "Image recognition captchas," in *Information Security*, K. Zhang and Y. Zheng, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 268–279. [Online]. Available: https://doi.org/10.1007/978-3-540-30144-8_23

[123] J. P. Bigham and A. C. Cavender, "Evaluating existing audio captchas and an interface optimized for non-visual use," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '09. New York, NY, USA: Association for Computing Machinery, 2009, p. 1829–1838. [Online]. Available: https://doi.org/10.1145/1518701.1518983

[124] M. Jain, R. Tripathi, I. Bhansali, and P. Kumar, "Automatic generation and evaluation of usable and secure audio recaptcha," in *The 21st International ACM SIGACCESS Conference on Computers and Accessibility*, ser. ASSETS '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 355–366. [Online]. Available: https://doi.org/10.1145/3308561.3353777

[125] K. Schwab. (2019) Google's new recaptcha has a dark side. [Online]. Available: https://www.fastcompany.com/90369697/googles-new-recaptcha-has-a-dark-side

[126] Brave. (2019) zksense: a privacy-preserving mechanism for bot detection in mobile devices. [Online]. Available: https://brave.com/zksense-a-privacy-preserving-mechanism-for-bot-detection-in-mobile-devices/

[127] S. I. Matthew Prince. (2020) Moving from recaptcha to hcaptcha. [Online]. Available: https://blog.cloudflare.com/moving-from-recaptcha-to-hcaptcha/

[128] R. A. Nachar, E. Inaty, P. J. Bonnin, and Y. Alayli, "Breaking down captcha using edge corners and fuzzy logic segmentation/recognition technique," *Security and Communication Networks*, vol. 8, no. 18, pp. 3995–4012, 2015. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.1316

[129] C. J. Hernández-Castro, S. Li, and M. D. R-Moreno, "All about uncertainties and traps: Statistical oracle-based attacks on a new captcha protection against oracle attacks," *Computers & Security*, vol. 92, p. 101758, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404820300420

[130] M. Mohamed, B. Shrestha, and N. Saxena, "Smashed: Sniffing and manipulating android sensor data for offensive purposes," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 4, pp. 901–913, 2017. [Online]. Available: https://doi.org/10.1109/TIFS.2016.2620278

Meriem Guerar received the Master degree in Information Systems and Networks from the University of Sciences and the Technology of Oran (USTO), Algeria, in 2011, and her Ph.D. in 2017. She is is currently working as a post-doc research fellow at the University of Genova, Italy. Her main research interests include the areas of authentication, security and usability, blockchain and smartphone security.

Luca Verderame obtained a Ph.D. in Electronic, Information, Robotics, and Telecommunication Engineering at the University of Genoa (Italy) in 2016, where he worked on mobile security. He is currently working as a post-doc research fellow at the Computer Security Laboratory (CSEC Lab), and he is also the CEO and Co-founder of Talos, a cybersecurity startup and university spin-off. His research interests mainly cover information security applied, in particular, to mobile and IoT environments.

Mauro Migliardi is Associate Professor at the University of Padua and Adjunct Professor at the University of Genoa. He is a member of the Scientific Committee of the Center for Computing Platforms Engineering, he has won the 2013 Canada-Italy Innovation Reward and he leads the joint CIPI-Gruppo Sigla s.r.l. Lab for CyberSecurity. He participated to several national and international research projects, chaired or co-chaired several international workshops and conferences and he is member of the Technical Program Committees of several international workshops and conferences and has tutored more than 200 Bachelor, Master and PhD students at the Universities of Genoa, Padua and Emory. His main research interest is distributed systems engineering in general; recently he focused on mobile systems, cybersecurity, green security, IoT security and human memory support services,. More details are available at http://geas.dei.unipd.it/migliardi/index.html.

Francesco Palmieri received the M.S. degree and the Ph.D. degree in computer science from the University of Salerno. He is a Full Professor at the University of Salerno. His research interests include advanced networking protocols and architectures and network security. He has been the director of the Networking Division of the University of Naples "Federico II" and contributed to the development of the Internet in Italy as a senior member of the Technical-Scientific Advisory Committee and of the CSIRT of the Italian NREN GARR. He serves as the editor-in-chief of an international journal and participates to the editorial board of other highly-reputed ones.

Alessio Merlo is an Associate Professor in Computer Engineering in the Department of Informatics, Bioengineering, Robotics and System Engineering Department (DIBRIS) at the University of Genoa, and a member of the Computer Security Laboratory (CSEC Lab). His main research field is Mobile Security, with a specific interest on Android security, automated static and dynamic analysis of Android apps, mobile authentication and mobile malware. More information can be found at: http://csec.it/people/alessio_merlo/