# УДК 004.89

# Подходы человеко-искусственного интеллекта для безопасного анализа в кодах

Костева Анна

ФГБОУ ВО Белгородский ГАУ, п. Майский, Россия

Аннотация

CAPTCHA (полностью автоматизированный общедоступный тест Тьюринга для различения компьютеров и людей) уже давно используется для предотвращения неправильного использования автоматизированными ботами веб-сервисов путем использования взаимодействия человеко-искусственный интеллект (HAI) для различения, является ли пользователь человеком или компьютерной программой. На протяжении многих лет предлагались различные схемы CAPTCHA, главным образом для повышения удобства использования и безопасности от появляющихся ботов и хакеров, выполняющих вредоносные операции. Однако автоматизированные атаки эффективно взломали все распространенные традиционные схемы, и большинство существующих методов CAPTCHA также уязвимы для ретрансляционных атак с участием человека. Невидимая рекапча и некоторые подходы еще не взломаны. Однако с появлением ботов четвертого поколения, точно имитирующих поведение человека, безопасная CAPTCHA вряд ли была бы разработана без дополнительных специальных устройств. Почти все основанные на когнитивных данных CAPTCHA с поддержкой датчиков еще не были скомпрометированы автоматическими атаками. Однако они по-прежнему подвержены ретрансляционным атакам с участием человека из-за ограниченного числа проблем и могут быть решены только с использованием надежных устройств. Очевидно, что схемы CAPTCHA, основанные на когнитивных данных, имеют преимущество перед другими схемами в борьбе с атаками на безопасность. В этом исследовании, в качестве надежной отправной точки для создания будущих безопасных и удобных схем CAPTCHA, мы предложили обзорный анализ HAI между пользователями компьютеров и компьютерами в аспекте безопасности открытых проблем, трудностей и возможностей текущих схем CAPTCHA.

1 Введение

CAPTCHA (Полностью автоматизированный публичный тест Тьюринга для различения компьютеров и людей) или HIP (Интерактивное доказательство человека) - это автоматический механизм безопасности, позволяющий отличить пользователя от человека или компьютерной программы. Он создает и оценивает тесты, которые могут быть решены людьми, но находятся за пределами возможностей современных компьютерных программ. Это превратилось в наиболее часто используемую стандартную меру безопасности для предотвращения автоматизированных атак на компьютерные программы. С ростом веб-сервисов атаки типа "Отказ в обслуживании" (DoS), осуществляемые вредоносными автоматизированными программами, стали серьезной проблемой, и тест Тьюринга стал решающим подходом для отличия людей от опасных автоматизированных программ. Судья-человек уполномочен задать ряд вопросов двум игрокам, один из которых был компьютером, а другой человеком, и отличить их друг от друга в оригинальном тесте Тьюринга. CAPTCHA, как и тест Тьюринга, отличает людей от компьютеров, но судьей теперь является машина. В общем, CAPTCHA - это криптографический протокол [[1](https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-022-00134-9#ref-CR1)], базовое предположение о надежности которого основано на задаче искусственного интеллекта. CAPTCHA подразумевает беспроигрышную ситуацию: либо captcha не взломана и есть способ отличить людей от компьютеров, либо captcha взломана, и сложная проблема искусственного интеллекта решена. CAPTCHA обычно представляет собой простой визуальный тест или головоломку, которую человек может выполнить без особых трудностей, но автоматизированная программа не может понять. Тест обычно состоит из букв, цифр или их комбинации с наложением и пересечением. Изображения CAPTCHA могут быть искажены или показаны на сложном фоне, что затрудняет их чтение программным обеспечением оптического распознавания символов (OCR). CAPTCHA имеет широкий спектр применений в Интернете и других приложениях, таких как черви и спам, онлайн-опросы, бесплатные почтовые сервисы, предотвращение атак по словарю, а также играет значительную роль в ограничении частоты использования.

HAI (искусственный интеллект человека) исследует взаимодействия между людьми и компьютерами, а также основные явления, которые их окружают. Он обозначает характеристики удобства использования, которые тесно связаны с пользовательским интерфейсом и человеческими факторами. Следовательно, он тесно связан с информатикой, искусственным интеллектом и когнитивной психологией. Основная концепция HAI - удобство использования. С этой точки зрения, такие головоломки, как CAPTCHA, которые люди могут легко решить, но компьютеры находят сложными, являются примером HAI. В этом исследовании мы представили обзорный анализ HAI в рамках аспектов безопасности открытых проблем, трудностей и возможностей текущих схем CAPTCHA. Оставшаяся часть этой статьи организована следующим образом: В разделе II представлена таксономия атак с использованием CAPTCHA. Раздел III описывает анализ проблем с CAPTCHA. В результате в разделе IV представлены предложения и рекомендации по созданию хорошей CAPTCHA. Наконец, раздел V завершает статью.

1.1 Эволюция CAPTCHA

Первый человек, Мони Наор [2], предложил теоретические подходы для отличия компьютеров от людей. В 1997 году веб-поисковой системе AltaVista приписывали то, что она первой использовала CAPTCHA в Интернете [3]. Текстовые CAPTCHA были ведущим методом в начале 2000-х годов. Был разработан набор атак с использованием алгоритмов обработки изображений, распознавания образов и машинного обучения (ML) для взлома популярных текстовых схем [4]. Кроме того, алгоритмы анти-распознавания и антисегментации были использованы в попытке улучшить безопасность существующих текстовых CAPTCHA. В 2014 году Google сообщила, что разработки в области технологии искусственного интеллекта могут разрешать искаженные варианты текста с 99,8% [5]. С 2004 года проблемы компьютерного зрения (CV), включая классификацию и распознавание изображений, считались более сложными задачами ИИ, чем распознавание текста. После этого появилось множество схем CAPTCHA на основе изображений с перетаскиванием, выбором изображения или скольжением, чтобы отличать людей от компьютеров. Однако передовые решения CV и ML помогли устранить наиболее важные схемы CAPTCHA, основанные на изображениях, в период с 2013 по 2018 год. Несколько схем CAPTCHA на основе изображений, таких как схема reCAPTCHA V2, были атакованы ML [6]. Кроме того, в качестве контрмер против моделей глубокого обучения были предложены такие подходы, как искажение, смешивание фонового шума и использование состязательных инстансов. Состязательные примеры, Сегеди и др. [7] и другие были предложены для повышения его защищенности от атак на основе ML [8,9,10]. Однако Na и др. [11] предложили решатель CAPTCHA, который использует постепенное обучение на ограниченном наборе данных, чтобы победить состязательные CAPTCHA. Для работы с пользователями с нарушениями зрения исследователи предложили звуковые CAPTCHA в дополнение к текстовым CAPTCHA и CAPTCHA на основе изображений. Однако языковые барьеры и плохое удобство использования ограничивают эффективность этих схем. Кроме того, контролируемое обучение и автоматическое распознавание речи (ASR) [12] показывают, как эти схемы могут быть использованы. Исследователи начали разрабатывать схемы CAPTCHA, основанные на поведении, в 2010-х годах, чтобы создавать трудности, основанные на поведенческих особенностях. Первая CAPTCHA, основанная на поведении, была запущена Geetest в 2012 году, в то время как Google выпустила No CAPTCHA reCAPTCHA в 2014 году и invisible CAPTCHA в 2015 и 2017 годах. Было продемонстрировано, что атаки ботов, имитирующих поведенческий паттерн пользователя, уязвимы для этих схем [6]. Из-за серьезных соображений конфиденциальности Cloudflare недавно решила прекратить использование reCAPTCHA [13]. Наконец, последние направления исследований используют данные датчиков для создания задач, которые трудно воспроизвести автоматизированным ботам. Однако мы должны подождать достаточное количество времени, прежде чем сможем полностью оценить CAPTCHA на основе датчиков.

1.2 Коды CAPTCHA

Схемы CAPTCHA различаются и постоянно совершенствуются в результате достижений в области передовых технологий, искусственного интеллекта и методов взлома. Основные коды CAPTCHA, показанные на рис. 1, в настоящее время классифицируются как основанные на когнитивных / поведенческих, видео-, аудио-, графических, текстовых и других.

Рис. 1



Основные схемы CAPTCHA

Изображение в натуральную величину

1.2.1 Текстовые CAPTCHA

С годами эти CAPTCHA стали применяться все чаще. В этих методах текст искажается и показывается пользователю в виде изображения, и пользователь должен точно ввести этот текст перед прохождением этого теста. Предположение о надежности ИИ заключается в том, что люди могут легко прочитать искаженный текст, но ботам, использующим методы оптического распознавания символов (OCR), это сложно. Различные варианты отображения текста задачи можно разделить на три подкатегории: 2D, 3D и анимация.

Капчи на основе 2D-текста

Андрей Бродер со своей командой из Исследовательского центра DEC Systems изобрел 2D-текстовую схему CAPTCHA в 1997 году. Аналогичный метод был использован веб-сайтом AltaVista для предотвращения влияния ботов на рейтинг сайтов в поисковой системе [24]. Фон Ан и Блюм создали Gimpy CAPTCHA и EZ-Gimpy [14] в сотрудничестве с Yahoo в 2000 году, чтобы предотвратить создание ботами вредоносной рекламы и бесплатных учетных записей. Gimpy CAPTCHA требует, чтобы вы правильно ввели по крайней мере три из семи случайных слов в словаре. EZ-Gimpy - это сокращенная версия Gimpy, которая случайным образом отображает только одно слово в словаре. В сгенерированных изображениях word используются различные шрифты, градиенты, шум и другие эффекты, затрудняющие их распознавание ботами. Моника Чу и Генри Бэрд предложили BaffleText [15] в 2003 году, текстовую КАПЧУ, использующую произносимые псевдослучайные слова с алгоритмами маскировки, чтобы предотвратить распознавание программным обеспечением OCR. Megaupload.com создал схему CAPTCHA, устойчивую к сегментации, в 2010 году. Этот метод использует перекрывающиеся символы, а также принцип “Восприятия гештальта”. Согласно принципу восприятия гештальта, люди могут мысленно реконструировать отдельные символы, в то время как компьютеры все еще с трудом справляются с этой задачей. Первая версия reCAPTCHA была разработана для защиты веб-сайтов от компьютерных атак. Если пользователь правильно введет известные слова из двух искаженных слов в старых книгах, он пройдет испытание. Чоу предложили концепцию текстовой интерактивной CAPTCHA. Их подход требует построения сетки кликабельных CAPTCHA из нескольких текстовых вызовов CAPTCHA. Пользователь должен выбрать элементы сетки, которые соответствуют требованиям задачи. Вместо использования текста, напечатанного на машинке, авторы предложили рукописные подписи, чтобы предотвратить распознавание программным обеспечением OCR.

3D текстовые CAPTCHA

Эти схемы CAPTCHA используют преимущества последовательностей распознавания символов 3D людьми, но боты не могут, что делает их превосходящими капчи на основе 2D текста. Исследовательская группа OCR разработала Teabag3D, высокозащищенную CAPTCHA. Эта CAPTCHA состоит из изображения, в котором текстовые символы сочетаются с 3D-рисунком. Super CAPTCHA и 3DCAPTCHA - это текстовые схемы CAPTCHA, использующие те же допущения, что и Teabag3D. С 2013 года Super CAPTCHA доступна в качестве WordPress.org плагин. Имсамаи и Фимолтарес разработали схему 3D CAPTCHA, которая включает в себя отображение 3D буквенно-цифровых последовательностей и смешивание множества эффектов, таких как наложение, поворот, шум, изменение шрифта, масштабирование и другие эффекты, чтобы обмануть распознавание автоматизированных ботов. Сьюзи недавно предложили DotCHA, КАПЧУ на основе 3D-текста. 3D-буквы в каждой задаче состоят из маленьких сфер. Каждая буква читается под разным углом поворота вокруг горизонтальной оси. В результате 3D-модели текста необходимо поворачивать несколько раз, чтобы идентифицировать их буквы.

Animated text-based CAPTCHAs

Эти CAPTCHA добавляют временное измерение к текстовым схемам. Подробно, текстовое содержимое анимировано в коротком ролике для каждой задачи, что усложняет извлечение для автоматизированных ботов. В 2006 году Фишер и Херфет предложили одно из первых анимированных предложений CAPTCHA. Концепция этой CAPTCHA заключается в проецировании текста на анимированную деформирующуюся поверхность. Науманн разработали анимированную CAPTCHA с идеей восприятия системы человеческого глаза в 2009 году. Только когда буквы перемещаются, пользователи могут отличить текст от фона. С той же концепцией Цуй и представили анимированную CAPTCHA, которая распознает правильные символы только при перемещении. Принцип “нулевой осведомленности на кадр” применяется для обеспечения отсутствия утечек информации в каждом кадре. В 2010 году Creo Group выпустила анимированную HelloCAPTCHA. Для каждой задачи последовательность из шести символов представлена в виде GIF-изображения с некоторыми эффектами: случайные позиции, различная ориентация и другие. Информация распределяется по нескольким кадрам, чтобы предотвратить распознавание по одному кадру. Проблема в NuCaptcha начинается с видеоролика с текстом, набранным белым шрифтом, за которым следуют три красных символа на динамическом фоне. Чтобы пройти испытание, пользователь должен правильно ввести красные символы. В Dracon CAPTCHAs пять символов отображаются в фиксированных местах, которые были случайным образом изменены с эффектами затухания, размытия и шума.

1.2.2 CAPTCHA на основе изображений

В связи с недавним сбоем почти текстовых CAPTCHA растет беспокойство по поводу их надежности защиты и доступности. В последнее время все больше проектов фокусируются на распознавании изображений, а не символов, исходя из предположения, что общие проблемы с видением сложнее, чем распознавание текста.  Интерактивные CAPTCHA

Эти CAPTCHA основаны на взаимодействии пользователя, таком как жесты пролистывания или движение мыши, чтобы выявить скрытые точки на изображении. Конти предложили CAPTCHaStar, в котором используется способность людей распознавать формы в загроможденной среде. Задача CAPTCHaStar состоит из белых пикселей, называемых звездочками, которые случайным образом перемешаны друг с другом. Положение этих звездочек меняется в зависимости от того, где находится курсор. Пользователи должны перетащить курсор так, чтобы звездочки образовали понятную форму, прежде чем нажать левую кнопку мыши, чтобы пройти тест CAPTCHA. Окада и др. создали Noise CAPTCHA с той же концепцией. Эта CAPTCHA состоит из двух изображений разного размера с зашумлением, а также скрытого объекта или сообщения на одном из изображений. Пользователи должны перетащить маленькое зашумленное изображение, чтобы идентифицировать скрытый объект на большом изображении, прежде чем нажать кнопку “Отправить”, чтобы пройти проверку CAPTCHA. CAPTCHA Cursor, предложенная Томасом отображает пять курсоров случайным образом на сгенерированном изображении. Чтобы пройти испытание, пользователи должны навести указатель мыши на определенный курсор.

Капчи на основе выбора

Эти CAPTCHA требуют, чтобы пользователи выбирали изображения-кандидаты из набора изображений. Для описания этой задачи может использоваться только текст или текст с образцом изображения. Asirra - типичная CAPTCHA этой схемы, в которой пользователям предлагается выбрать всех кошек из набора из 12 изображений собак и кото. В HumanAuth CAPTCHA пользователи должны выбирать все изображения, содержащие естественный контент, среди изображений естественного контента (таких как дерево или река) с изображениями искусственного контента (такими как автомобиль или часы). CAPTCHA SEMAGE (СЕмантически сопоставляющие изображения) отличается от Asirra и HumanAuth CAPTCHA тем, что требует от пользователей выбирать семантические изображения из набора изображений. В результате пользователь должен сначала распознать содержимое каждого изображения, а затем определить семантическую взаимосвязь между ними. Google выпустила “No captcha reCAPTCHA” в 2014 году. Анализируя среду браузера (например, файлы cookie и историю браузера), система определяет, столкнулась ли она с ботом или нет. На странице будет отображаться только флажок или КАПЧА на основе выбора в зависимости от уровня риска. В результате проверки CAPTCHA на основе выбора отображаются девять изображений-кандидатов и образец изображения, описывающий требуемое содержимое изображения. Чтобы пройти испытание, пользователь должен выбрать изображения, похожие на образец. Изображение CAPTCHA Facebook похоже на reCAPTCHA по своему подходу. Чтобы выполнить задание, пользователи должны выбрать изображения, соответствующие описанию подсказки, из набора из двенадцати изображений с различным содержанием. Avatar CAPTCHA предлагает пользователям выбрать лица аватара из набора из 12 изображений в оттенках серого, которые включают лица человека и аватара. FR-CAPTCHA и FaceDCAPTCHA - это еще две капчи для изображений лиц. FR-CAPTCHA требует, чтобы пользователи выбирали два изображения лица одного и того же человека на сложном фоне. С другой стороны, в FaceDCAPTCHA пользователи должны выбирать между визуально искаженными изображениями человеческих лиц и изображениями нечеловеческих лиц.

Капчи на основе кликов

Эти схемы отображают текст и изображение, адрес которых пользователь должен щелкнуть, чтобы пройти испытание. Основным ограничением этого типа является то, что для создания нового экземпляра требуется вмешательство человека. Неявная CAPTCHA является распространенным примером, который требует, чтобы пользователи нажимали на идентичное местоположение изображения. Тан первыми применили SACaptcha, в котором пользователи должны щелкнуть по некоторым областям CAPCHA, связывающим объясненную конкретную форму, чтобы пройти испытание.

Капчи на основе рисования

В 2006 году Ширали-Шахреза, первый человек, разработал Drawing CAPTCHA КАПЧУ на основе рисунка. Ромбовидные точки соединены линиями, нарисованными пользователем. Наиболее сложным аспектом является то, что пользователи должны идентифицировать эти точки на фоне шума. VAPTCHA (публичный тест Тьюринга на основе вариационного анализа, позволяющий отличить компьютеры от людей) состоит из изображения со случайно сгенерированной траекторией в задании. Чтобы выполнить задачу, пользователи должны нарисовать траекторию, совпадающую с этой траекторией. В MotionCAPTCHA аналогично пользователям также предлагается нарисовать фигуру, аналогичную той, что отображается в окне запроса.

Капчи на основе слайдов

В этих CAPTCHA для решения задачи пользователи должны использовать ползунок, например, перетащить фрагмент изображения в нужное место, повернуть ориентацию изображения или выбрать правильную форму изображения. ЧТО НОВОГО CAPTCHA отображает три повернутых изображения случайным образом, и пользователи должны повернуть изображения в правильное положение. CAPTCHA Minteye Slide-to-Fit отображает закрученное изображение, и пользователи должны перемещать предоставленный ползунок, пока не увидят неискаженную версию изображения. Tencent CAPTCHA требует, чтобы пользователи перемещали ползунок, чтобы сопоставить две части головоломки.

Капчи на основе перетаскивания

В этих CAPTCHA пользователи должны выравнивать фрагменты изображения, чтобы сформировать полное изображение, перетаскивая их. Garb CAPTCHA отображает четыре случайно перетасованных фрагмента изображения. Пользователи должны изменить порядок этих фрагментов изображения, чтобы получить полное изображение для прохождения теста CAPTCHA. Хамид Али впервые использовали CAPTCHA на основе головоломок. Для завершения задачи требуется перетащить четыре фрагмента изображения в пустую сетку из четырех ячеек. Гао предложили CAPTCHA, основанную на изображениях, на основе головоломки. В этой CAPTCHA изображение разделено на множество частей (например, 9, 16 или 25), причем только две части расположены неправильно. Пользователи должны поменять местами неправильные фрагменты, чтобы решить проблему. Capy CAPTCHA требует, чтобы пользователи перемещали кусочек головоломки в недостающее место в задании. Это недостающее место заполнено случайной частью изображения. KeyCAPTCHA отображает три части головоломки и неполное изображение. Пользователи должны собрать эти фрагменты в соответствии с эталонным изображением. Как только курсор останется во фрейме, эталонное изображение исчезнет. Чтобы пройти испытание CAPTCHA, пользователи должны переместить эти фрагменты в правильные места.

1.2.3 Аудио-капчи

Для людей с нарушениями зрения предложенной альтернативой схемам визуальной CAPTCHA были схемы CAPTCHA на основе звука. Они должны ввести то, что они услышали, чтобы пройти тест. В Университете Карнеги-Меллон исследователи представили аудио reCAPTCHA, приобретенный Google позже. Чтобы решить проблему, пользователи должны идентифицировать восемь цифр, произносимых в человеческом шуме, и принять только одну неправильную цифру в этих цифрах. Аудио-КАПЧА eBay состоит из шести цифр, произносимых различными шумными голосами. Капчи Microsoft состоят из десяти цифр, произносимых разными голосами, смешивающими шум некоторых разговоров. Yahoo CAPTCHA требует от пользователей ввода семи цифр после трех звуковых сигналов, произносимых ребенком, на фоне шума. Версия Audio reCAPTCHA 2013 года требует, чтобы пользователи распознавали все цифры, разделенные на три группы в задаче. В каждом кластере встречаются три или четыре перекрывающиеся цифры. Новая версия reCAPTCHA в 2017 году включала десять произносимых цифр и фоновый шум.

1.2.4 Капчи на основе видео

В задаче создается короткое видео, отражающее определенный контент, пользователи должны понять и описать его текстом.  Клювер предложили CAPTCHA, в котором пользователи должны просмотреть короткое видео, а затем ввести три слова для его описания. Ширали-Шахреза и др. предложили Motion CAPTCHA, которая требует, чтобы пользователи описывали движение человека во время просмотра видео, выбирая одно из предложений.

1.2.5 CAPTCHA, основанные на когнитивных данных

Методы CAPTCHA, основанные на когнитивных способностях, которые обеспечивают повышенную безопасность, в значительной степени заменили традиционные методы Captcha. Когнитивные способности - это навыки, основанные на мозге, которые являются результатом четкой комбинации нейробиологических и психологических методов. Знания, концентрация, память, суждения и оценка, рассуждения и вычисления, решение проблем и принятие решений - все это аспекты человеческого познания и поведения. Чтобы отличить людей от ботов, эти методы CAPTCHA используют биометрические (то, чем вы являетесь), физические (то, что у вас есть) и основанные на знаниях (то, что вы знаете) факторы с поддержкой или без поддержки таких датчиков, как гироскоп или акселерометр. В таблице мы перечисляем наиболее распространенные CAPTCHA, основанные на когнитивных данных. В 2020 году Асьен предложили BeCAPTCHA-Мышь, которая отличает людей от ботов, анализируя траектории мыши во время вызова. Gametrics проводит различие между людьми и ботами, собирая и анализируя движения мыши пользователя во время операций перетаскивания для решения динамической когнитивной игры. GEETest и Netease, как и Tencent CAPTCHA, требуют, чтобы пользователи заполняли КАПЧУ на основе скользящего изображения, перемещая ползунок до тех пор, пока не будут подобраны две части головоломки. Если пользователи завершают проверку и их поведение при скольжении не вызывает подозрений, считается, что они прошли проверку. Сирипитакчай и др. предложили EYE-CAPTCHA, в которой пользователи должны решать математическую задачу, двигая глазами. Чтобы выполнить задание, пользователь должен определить правильный ответ и глазами переместить ответ в центр экрана. В 2014 году Google запустил “No CAPTCHA reCAPTCHA” (reCAPTCHA V2). Все, что требуется, это установить флажок “Я не робот”. Однако поведение пользователя (такое как щелчок, перемещение мыши и другое поведение) наряду с другой информацией (браузер, файлы cookie, история и т.д.) Собирается и анализируется в фоновом режиме. Если пользователи подозреваются в том, что они боты, им необходимо заполнить вторую рекапчу на основе изображений. В 2017 году была выпущена Invisible reCAPTCHA, обновленная версия reCAPTCHA V2. Процесс оценки инициируется в фоновом режиме путем запуска вызова JavaScript API или нажатием пользователями существующей кнопки. Невидимый reCAPTCHA, как и подход “Без CAPTCHA reCAPTCHA”, требует повторного тестирования reCAPTCHA на основе изображений, если пользователи подозреваются в том, что они боты. В 2015 году Герар, первый человек, представили физическую CAPTCHA для мобильных устройств, названную CAPPCHA (Полностью автоматизированный общедоступный физический тест, позволяющий отличать компьютеры от людей). Пользователи должны наклонять устройство до определенной степени, что сложно сделать ботам. Хупперих в 2016 году была введена сенсорная CAPTCHA, в которой пользователи должны выполнять сложные жесты (например, ловить рыбу, бить молотком, пить) с помощью своих мобильных устройств. Авторы предложили шагометрическую CAPTCHA, в которой люди должны пройти не менее пяти шагов. Когда пользователь идет, в мобильном устройстве генерируется ускорение, затрудняющее работу ботов. Мантри предложили схему CAPTCHA, в которой пользователи должны выполнять требование перемещения устройства в соответствии с конкретным руководством, отображаемым на устройстве. Фрэнк инструктировали пользователей выполнять обнаруживаемый жест и распознаваться гироскопом (например, вращение, наклон или рисование) при перемещении устройства. Герар и др. разработали невидимую CAPPCHA, которая похожа на CAPPCHA в том, что задача невидима для пользователей.Считывающие датчики обнаруживают нажатия пользователя в отличие от событий на сенсорном экране, которые боты могут легко имитировать. Кроме того, эта CAPTCHA защищает конфиденциальность пользователя, не отправляя конфиденциальные данные на сервер. AccCAPTCHA требует, чтобы пользователь играл в игру rolling ball. Чтобы завершить игру, пользователь должен управлять мячом с помощью датчиков движения устройства. GISCHA, КАПЧА на основе игр для мобильных устройств, была предложена Янгом. Чтобы пройти испытание, пользователь должен переместить мяч в правильную лунку. Абабтейн и др. предложили CAPTCHA, которая требует от пользователей прохождения простой игры с использованием датчиков. Они предложили пять игр, в каждой из которых было несколько статичных и один движущийся объект. Пользователи должны перемещать движущийся объект, чтобы попасть в правильные целевые статические объекты, чтобы пройти испытание. SenCAPTCHA был предложен Фенгом для определения местоположения ключевой точки на лице животного. Пользователям показывается маленький красный шарик и изображение животного. Затем они должны направить красный шарик в центр глаза животного, наклоняя свои устройства. Авторы предложили BrightPass, капчу мобильной аутентификации для защиты PIN-кода / пароля.Предлагаемый ими механизм использует яркость экрана, которую не могут обнаружить автоматизированные боты, чтобы определить, когда пользователи должны вводить правильную цифру или вводящую в заблуждение цифру. В виде физической CAPTCHA авторы предложили КАПЧУ аутентификации на основе PIN-кода, используемую для смарт-часов.Этот механизм основан на той же концепции, что и CAPPCHA. Для ввода пароля панель должна быть физически повернута на определенный градус. Аналогичным образом авторы используют вращение цифровой заводной головки в умных часах для защиты PIN-кода.

1.2.6 Другие типы

Стефан Поповенюк предложил метод аутентификации SpeakUp для удаленного голосования без присмотра в 2010 году. Голосовая биометрия улучшена с помощью текстовой КАПЧИ. Избиратели должны зачитать вслух характеристики проголосовавшего кандидата, отображаемые с помощью 2D-текстовой КАПЧИ. Кроме того, биометрические характеристики голоса избирателей определяются с помощью вызова. Автор также предложил записать видео избирателя о решении задач. Для защиты систем аутентификации по лицу Узун предложили rtCaptcha, КАПЧУ реального времени. Пользователи должны записать свое произношение вслух представленной 2D текстовой CAPTCHA.

Список литературы

1. М. Наор. Проверка человека в цикле или идентификация с помощью теста Тьюринга, [http://www.wisdom.weizmann.ac.il /~naor/PAPERS/human.ps](http://www.wisdom.weizmann.ac.il/~naor/PAPERS/human.ps).