Название статьи - "Подход человека и искусственного интеллекта к безопасному анализу кодов CAPTCHA". Статья рассматривает CAPTCHA и Human-AI Interaction (HAI) как механизмы безопасности, предназначенные для различения между людьми и компьютерами. CAPTCHA представляет собой криптографический протокол, создающий тесты, решаемые людьми, но сложные для компьютеров, с целью предотвращения атак и взломов. HAI исследует взаимодействие между людьми и компьютерами с учетом аспектов удобства использования и безопасности в рамках существующих схем CAPTCHA.

Исходные теоретические подходы к отличию компьютеров от людей, начиная с использования текстовых CAPTCHA в Интернете с 1997 года, привели к разработке различных схем, таких как текстовые и визуальные CAPTCHA. Эти схемы используются для защиты от атак и взломов, основанных на обработке изображений и алгоритмах машинного обучения. CAPTCHA, разработанные для различения человека от компьютера, эволюционировали от искаженного текста до более сложных форм, включая 3D-текст и анимированные текстовые CAPTCHA. Они созданы для усложнения задачи распознавания для компьютерных программ и ботов, однако они также вызывают проблемы конфиденциальности и удобства использования для пользователей.

Текстовые CAPTCHA стали менее надежными, и на смену им пришли изображения, требующие от пользователя различных действий, таких как движения мыши, выбор, клики, рисование, слайды или сборка головоломок. Для пользователей с нарушениями зрения предложены звуковые CAPTCHA, такие как звуковая reCAPTCHA, которая требует распознавания цифр в шуме. Видеоролики также используются, где пользователи должны описать содержание видео текстом или выбрать соответствующее предложение. Методы CAPTCHA, основанные на когнитивных способностях и включающие биометрические и физические факторы с использованием датчиков, предоставляют повышенную безопасность, заменяя традиционные методы CAPTCHA. Текстовые CAPTCHA, такие как Gimpy и EZ-Gimpy, подверглись успешным атакам, в том числе с использованием алгоритма корреляции, алгоритма прямой оценки искажений, машинного обучения, нейронных сетей и алгоритмов SIFT. Эти атаки демонстрировали уязвимости различных схем CAPTCHA, их успешность достигала 99%. Исследования выявили успешные атаки на разнообразные CAPTCHA на основе изображений, включая HumanAuth, Facebook, Google, reCAPTCHA V2, Tencent и другие. Методы атак включают в себя машины опорных векторов (SVM), атаки по побочным каналам, конволюционные нейронные сети (CNN), а также техники, использующие длину краев изображения и сжатие JPEG. Эти атаки подчеркнули уязвимость систем CAPTCHA к автоматизированным взломам. В 2009 году Филипп Голле представил эффективные атаки на ASIRRA, основанные на анализе особенностей CAPTCHA, таких как шрифт, форма, текстура и цвет. Этот метод обработки изображений разделяет фотографии на ячейки с текстурой и цветом, затем подается на классификаторы опорно-векторной машины (SVM) с успешной классификацией на уровне 83%. Эксперименты с использованием метода SVM и декодера Decaptcha продемонстрировали успешные атаки на аудио CAPTCHA, включая reCAPTCHA, с коэффициентами успешности от 45% до 85,15%. Эти атаки включали анализ волнового файла с использованием дискретного преобразования Фурье, алгоритм контролируемого обучения, скрытые марковские модели (HMM) и минимальное фонетическое отображение. Любая предвзятая идея в дизайне CAPTCHA, лишенная случайности, может стать объектом атак, таких как анализ побочных каналов или категоризации задач. Например, в Teabag неравномерное распределение размеров букв имеет уязвимость к атакам на фронтальные границы и обнаружение задней границы через корреляцию пикселей. Простые алгоритмы, такие как непрерывность пикселей, могут выявить фоновые области. Megaupload CAPTCHA, использующая фиксированный шрифт и углы поворота, становится уязвимой для анализа. Некоторые системы CAPTCHA подвержены обходу через использование ранее использованных идентификаторов сессии, ошибочной реализации кодирования ответов в URL или поле формы, а также других уязвимостей, таких как отправка клиенту хэша ответа. Ограниченные или неравномерно распределенные пулы задач и рискованные методы связи с сервером CAPTCHA также могут создавать потенциальные угрозы безопасности.

CAPTCHA превратилась в наиболее популярную стандартную меру безопасности для предотвращения автоматизированных атак компьютерных программ. В отличие от традиционных схем CAPTCHA, новые сенсорные и поведенческие схемы вызывают проблемы с конфиденциальностью, такие как отправка данных о поведении пользователя, файлов cookie и сенсоров на удаленные серверы. Это поднимает вопросы безопасности и требует внимания к конфиденциальности пользователей при разработке. С ростом автоматизированных атак становится проблемой различение между людьми и ботами в схемах CAPTCHA. Для усиления безопасности необходимо внедрение дополнительных мер, таких как оценка качества и поведения "флумана". Важно также различать алгоритмы "флуманов" и "помощи флуманов" и принимать меры против атак ретрансляции. Также следует рассмотреть методы предотвращения атак на фермы флуманов.

Подводя итог, CAPTCHA представляет собой схему безопасности, где конкурируют человек и компьютеры. В этом противостоянии человек полагается на сложность искусственного интеллекта. Однако развивающиеся технологии позволяют компьютерам эффективно решать сложные задачи искусственного интеллекта, что вызывает необходимость постоянного усовершенствования CAPTCHA.