Секция
«Современные проблемы в области математики, физики и информатики»

УДК 004.415.538

Кайсаров Д.К., магистрант, **Насс О.В.**, руководитель, доцент, доктор пед.наук, академик РАиО
Западно-Казахстанский аграрно-технический университет имени Жангир хана, г. Уральск, РК

ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ В СОЦИАЛЬНЫХ СЕТЯХ С ПОМОЩЬЮ ТЕСТА CAPTCHA ОТ СПАМ-РОБОТОВ В ВЕБ-ПРИЛОЖЕНИЯХ

Аннотация

В статье приведены данные по идентификации пользователей в социальных сетях с помощью теста CAPTCHA от спам-роботов в веб-приложениях.

Ключевые слова: *CAPTCHA, спам-робот, социальные сети, веб-приложения, идентификации пользователей.*

В настоящее время спам-роботы делятся на автоматические, которым сложно обойти систему капчу, и на полуавтоматические, которые могут взломать систему капчу.

CAPTCHA – стандартный механизм защиты сайтов от большинства существующих вредоносных программ. Поскольку CAPTCHA играет такую жероль, что и простейший протокол типа «запрос-ответ» (рисунок 1), эти тесты уязвимы для атак протокольного уровня — спамер переносит задачу решения тестов CAPTCHA для посетителей порносайтов либо передать ее на «аутсорсинг»(передача стороннему подрядчику ряда внутренних услуг и (или) сервисов компании-заказчика, в том числе на основе использования (например, аренды) его программных продуктов, приложений, технических средств и фрагментов инфраструктуры) в страну с дешевой рабочей силой.

Запрос-ответ. В семейство протоколов, называемых обычно по процедуре проверки "запрос-ответ", входит несколько протоколов, которые позволяют выполнить аутентификацию пользователя без передачи информации по сети. К протоколам семейства "запрос-ответ" относится, например, один из наиболее распространенных – протокол CHAP (Challenge-Handshake Authentication Protocol) [1].

Процедура проверки включает как минимум четыре шага (рисунок 1):

– пользователь посылает серверу запрос на доступ, включающий его логин;
– сервер генерирует случайное число и отправляет его пользователю;
– пользователь шифрует полученное случайное число симметричным алгоритмом шифрования на своем уникальном ключе (см. "Современные алгоритмы шифрования", "BYTE/Россия" № 8'2003), результат зашифрования отправляется серверу;
– сервер расшифровывает полученную информацию на том же ключе и сравнивает с исходным случайным числом. При совпадении чисел пользователь считается успешно аутентифицированным, поскольку признается владельцем уникального секретного ключа.

Реализация подобных атак зависит от архитектуры системы, например, хакеры способны обходить некоторые из ранних реализаций CAPTCHA путем перебора всех идентификаторов сеанса изображений с тестами.

Для взлома ранних текстовых вариантов CAPTCHA применяются специализированные алгоритмы компьютерного зрения. Например, Грег Мори и Джитендра Малик разработали сложные алгоритмы распознавания объектов, взламывающие с долей успеха в 95% тесты EZ-Gimpуис точностью 33% - тесты Gimpy.Данные схемы CAPTCHA разработаны в Университете

Карнеги-Меллона. Гэбриел Мой с коллегами позднее создали методики оценки искажений, которые позволили взламывать EZ-Gimpy в 99% случаев и Gimpy-r в 78% случаев.

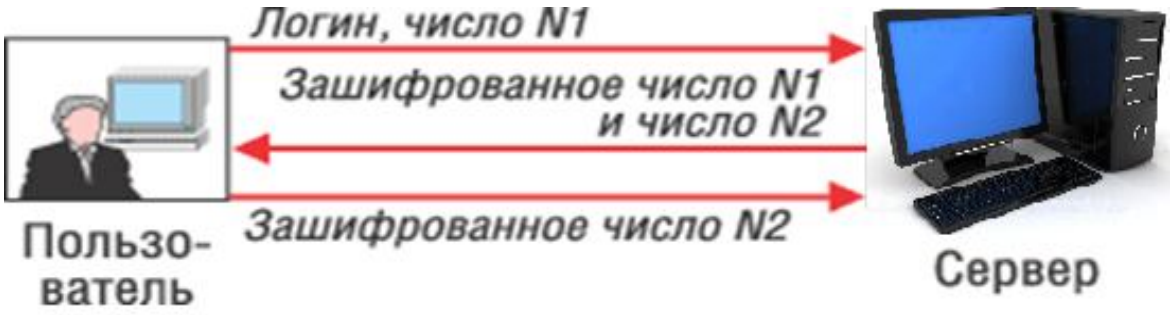

Рисунок 1 – Схема протокола аутентификации типа "запрос-ответ"

Идентификация местонахождения символов и порядка их следования, или сегментация, остается нерешенной проблемой, трудной с вычислительной точки зрения, а нередко и с комбинаторной. Поэтому исследователи предположили, что устойчивые текстовые схемы должны полагаться именно на трудность определения положения каждого символа, а не на сложность их распознавания.

Общий метод оценки устойчивости CAPTCHA состоит в следующем: если обозначить через s среднюю долю тестов, которые можно целиком верно сегментировать, а достижимый уровень распознавания индивидуальных символов — через r, то приблизительный общий уровень успеха взлома схемы рассчитывается по формуле $s*r^n$, где n — средняя длина используемых в схеме символьных последовательностей.

Набор символов, применяемых в CAPTCHA, также влияет на защищенность. Если обозначить размер набора символов через c, то вероятность слепого разгадывания теста с произвольной строкой из n символов будет равна $1/c^n$. Если в схеме употребляются только английские слова, то атакующий может попытаться собрать их все для организации словарной атаки, доля успешных попыток которой рассчитывается по формуле 1/w, где w — количество слов в словаре. Общепринятый критерий защищенности CAPTCHA, используемый при разработке тестов, таков: уровень успеха атак не должен превышать 0,01%, но при этом доля успешных попыток решения теста человеком должна составлять по меньшей мере 90%. Таким образом, между стойкостью CAPTCHA и читаемостью теста необходим определенный компромисс [1].

Другой способ взлома плохо проработанной защиты CAPTCHA – повторное использование идентификаторов сессии. В данном случае человек или программа-взломщик сначала вводит правильное значение CAPTCHA. Затем идентификатор сессии и ответ на CAPTCHA передается боту, который создает большое количество запросов с этим идентификатором, но с разными именами пользователя. Этот процесс можно продолжать до тех пор, пока не закончится срок действия идентификатора сессии.

Существует множество разновидностей капчи. Например: Во-первых, количество символов в записи. Во-вторых, для каждой позиции символа необходимо знать количество вариантов. В-третьих, имеются правилапостроения, т.е. с повторениями или без повторений построение комбинации. Для наглядности расчета следует рассмотреть на примере капчи с сервиса отправки смс через Интернет одного из операторов связи.

Капча состоит из 5 символов, которые могут быть как буквами латинского алфавита, так и цифрами. С математической точки зрения, комбинации символов являются размещениями с повторениями или конечными последовательностями. Их значение определяется как: количество элементов в степени равной числу элементов в наборе.

В этом случае число используемых букв равно 26 и число цифр равно 10, т.е. общее число элементов равно 36, тогда вариантов комбинаций будет 36 в степени 5 и соответствует 60 млн. 466176 комбинаций.

Возможность взлома – это перебор компьютером всех этих комбинаций. Т.о. теперь можно понять, как много нужно будет перебрать знаков, чтобы вручную подобрать символы.

Централизация базы пользователей. С постепенной «социализацией» Интернета, множество сайтов стали предлагать пользователям зарегистрироваться и взаимодействовать друг с другом. Публикация данных на сайт обычно проводится наряду с регистрацией полноценного аккаунта, или же анонимно. Оба этих метода являются открытыми воротами для спама. Социальная сеть Facebook анонсировал Facebook Connect, сервис, который предоставляет сайтам и их пользователям интегрированную платформу на базе социальной сети. Twitter подхватил эстафету с похожим сервисом «Войти с помощью Twitter». Оба этих сервиса могут быть встроены на сайт весьма легко, с их помощью можно полностью избавиться от регистрации и форм для комментариев, которые являются целью ботов. В качестве примера можно привести сервис *Janarin,* показано на рисунке 2.

Рисунок 2 – Сервис *Janarin*

Сервис *Janrain* предоставляет свое собственно решение, базированное на вышеупомянутых Facebook Connect, Sign in with Twitter и иже с ними, для того, что бы сделать сайт доступным из любой социальной сети.

Определение друзей. Еще одна CAPTCHA, представленная в январе 2011 года как результат работы Facebook. Компания экспериментирует с социальной аутентификацией для подтверждения владения аккаунтом. В чем же заключается этот эксперимент: Покажет вам несколько фотографий ваших друзей и попросит вас назвать того, кто на них изображен, (показано на рисунке 3). Хакеры могут знать ваш пароль, но не могут знать ваших друзей.

Тест Facebook на определение друзей. То, что делает нововведение Facebook абсолютно отличным от остальных решений, так это то, что эта CAPTCHA отсеивает не только роботов, но и вполне себе человечных злоумышленников.

У Facebook определенно есть перспектива внедрить эту CAPTCHA по всему Интернету. С базой в 600 миллионов пользователей и миллионами сайтов, в которые интегрированы модули Facebook, социальная сеть может использовать метод определения друзей для аутентификации где угодно.

Есть только одна проблема. Зачастую запросы дружбы – предмет обмена между пользователями для повышения заветной циферки, отражающей количество друзей. Когда этот список полон абсолютно неизвестных вам персон – едва ли возможно пройти этот тест.

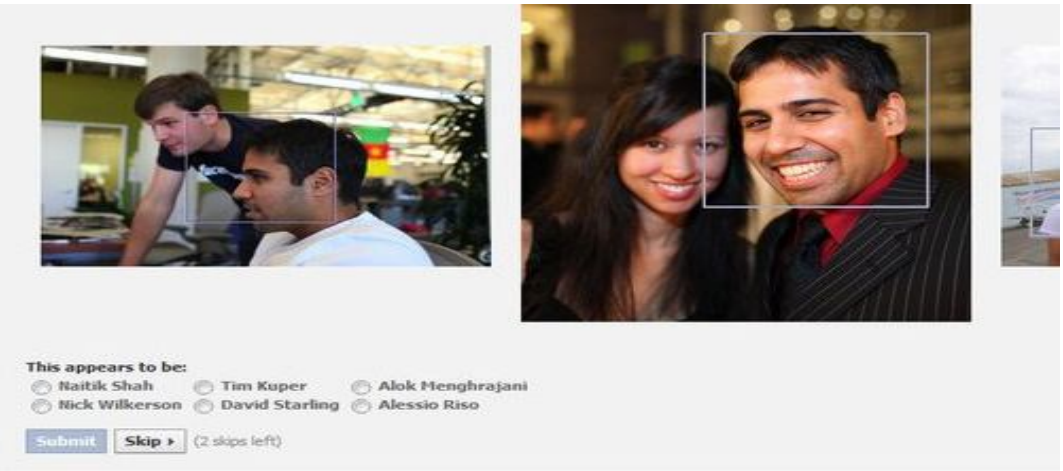

Рисунок 3 – Определение друзей

Интерактивные CAPTCHA. They Make Apps представила CAPTCHA в виде маленького ползунка, который надо передвинуть в правую сторону для того, чтобы подтвердить отправку данных. CAPTCHA сообщает пользователю: «Покажи свою человечность переведи ползунок на конец линии для создания аккаунта». They Make Apps использует CAPTCHA в виде ползунка. Этот вариант не подходит для людей с ограниченными способностями. Более того, разработка скрипта, который автоматически бы переводил ползунок для активации кнопки «Отправить» не должна быть сложной. Более продвинутая версия ползунка используется в комментариях в блоге Adafruit. Четыре разных ползунка должны быть установлены в правильное положение для публикации комментария [3].

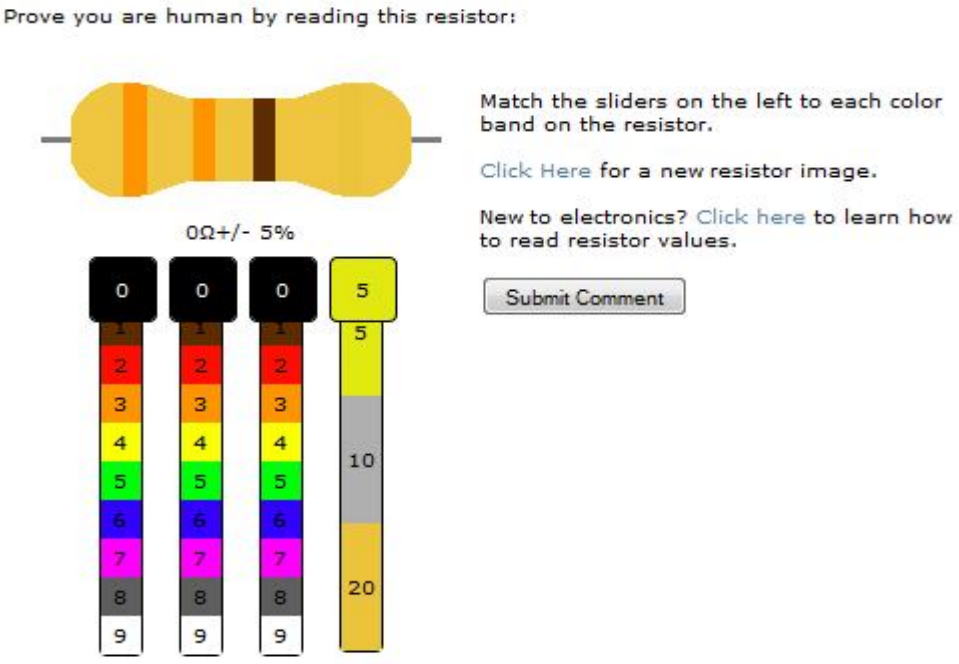

Рисунок 4 – Пример интерактивного теста

Интересный подход к борьбе против спама был продемонстрирован разработчиками keycaptcha.com. Метод заключается в том, что пользователю предоставляется возможность собрать простой пазл, пример приведен на рисунке 5. После чего системой анализируется изображение и в зависимости от этого пользователю позволяют/не позволяют доступ к другим действиям.

Рисунок 5 – Капча-пазл

СПИСОК ЛИТЕРАТУРЫ

1 Сергей Панасенко, Протоколы аутентификации, [Электронный ресурс]-URL:http://www.bytemag.ru/articles/detail.php?ID=9059;

2 Ахмад Салах Эль Ахмад, Джефф Ян, Перспективы повышения устойчивости CAPTCHA [Электронный ресурс] -URL:http://www.osp.ru/os/2011/02/13007706/;

3 Bushell, D., В поисках идеальной CAPTCHA [Электронный ресурс] / David Bushell// Mirapolis Virtual Room - система для проведения веб-конференций, презентаций, онлайн-обучения, совещаний и др.- URL: http://habrahabr.ru/post/120851/, http://timkadlec.com/2011/01/death-to-captchas/.

ТҮЙІН

Мақала веб қосымшаларда спам-боттардан сынақ SARTSNA пайдаланып әлеуметтік желілерде пайдаланушылардың сәйкестендіру туралы деректер ұсыналады.

RESUME

The article presents data on the identification of users in social networks using the test SARTSNA from spam bots in Web applications.

УДК 53.072:519.622.(0.63)

Маннапова Т.М.[1], ст. преп.,магистр, **Касымова А.Х.**[1], канд. пед.наук, доцент, Академик МАИН, **Даулетова А.Х.**[2], канд. пед.наук, доцент, Академик МАИН
[1]Западно-Казахстанский аграрно-технический университет им.Жангир хана, Уральск, Казахстан
[2]Евразийский национальный университет имени Л.Н. Гумилева, г.Астана, Казахстан

ВЗЛЕТ И ПАДЕНИЕ CAPTCHA

Аннотация

В данной статье рассмотрены проблемы о CAPTCHA. О том, что CAPTCHA сегодня полезна для веб-администраторов, но система очень устарелая и даже обновленные решения не долгосрочны, в будущем в течение 50 лет компьютеры разрушат любые формы CAPTCHA, т.е. роботы могут их распознать очень быстро.

***Ключевые слова**: CAPTCHA, интернет-сайт, социальные сети, спам, компьютер.*

В последнее время большинство интернет-сайтов использовуют CAPTCHA. Популярность CAPTCHA объясняется тем, что владельцам сайтов приходиться обеспечивать защиту от автоматической регистрации и рассылки спам сообщений. CAPTCHA (от англ. «Completely Automated Public Turing test to tell Computers and Humans Apart») представляет