УДК 621.326
Бреус В.
Одеський національний університет ім. І.І.Мечникова
Одеський національний морський університет

РОЗРОБКА СУЧАСНОГО ЗАХИСТУ WEB-САЙТІВ ВІД АВТОМАТИЧНОІ РЕЄСТРАЦІЇ

Вже багато років в мережі Internet розповсюдженим явищем є спам. Великої шкоди завдає не тільки небажані повідомлення, що розповсюджуються по електронній пошті, а й повідомлення, які спам-боти залишають на веб-сайтах – в форумах, в комментаріях до новин тощо. Першими кроками було введення обов'язкової реєстрації користувачів, але лише реєстрація не є ефективною мірою боротьби проти такого спаму. Сьогодні майже завжди при розробці реєстраційних форм використовують CAPTCHA (автоматичний тест Тьюринга для розпізнання комп'ютерів та людей).

Розроблені різні варіанти тесту. Найбільш розповсюджені – графічний, коли є зображення, текст з якого потрібно ввести в поле, та логічний, коли користувачу запропоновано відповісти на якесь нескладне запитання. На теперішній час ці тести легко обходять. Зазвичай кількість запитань в логічних тестах скінченна, легко можна отримати весь набір питань та скласти список відповідей. Графічна CAPTCHA теж не є ідеальним захистом від автоматичної реєстрації. Якщо символи відображаються в неспотвореному вигляді та без шуму – вона легко розпізнається за допомогою програмного забезпечення для розпізнавання символів, а якщо навпаки – людина не може розпізнати зображення. Також можуть бути використані сервіси розпізнавання зображень, в яких одні люди розпізнають зображення для інших людей. Не рідкістю є випадки, коли відповідь на питання або текст з зображення передається клієнту в незашифрованому вигляді в cookies тощо.

Що ж потрібно для максимального захисту? По перше, необхідно розробити скрипт, що ускладнить роботу програмного забезпечення для автоматичної реєстрацій. Назви полів форми в HTML-коді повинні бути випадковими, змінної довжини, та зберігатись на сервері для подальшої перевірки. HTML-код повинен бути розроблений таким чином, щоб програмними засобами було неможливо встановити відповідність між назвами та смислом полів. Подібний захист використовується сайтами mail.ru та i.ua, але там легко відрізнити назви полів форми. По друге, необхідно створити зображення, що може бути розпізнене людиною, але не програмним забезпеченням. Найкращий варіант – помірно спотворені символи різних близьких кольорів що обов'язково трохи перекривають один одного на неоднорідному фоні. Також потрібно забезпечити захист від розпізнавання зображення робітником сервісу розпізнавання зображень. Одним з можливих методів є таймаут – короткий проміжок часу, після якої CAPTCHA стає недійсною, але це не ідеальний та не зручніший для користувачів варіант.

Я пропоную замість звичайної послідовності символів або математичної формули використовувати нескладне завдання. Приклад - розташувати букви або цифри у зростаючому або спадаючому порядку, ввести лише букви або ввести лише символи одного кольору. Символи будуть розташовані на зображені у довільному порядку, а текст завдання описаний поза зображенням. Завдання обирається випадковим чином. В розробці рішення, що відповідає описаним критеріям. Після тестування на одному з існуючих веб-сайтів цей алгоритм буде взятий за основу для створення публічної системи для захисту українських веб-сайтів (аналог reCaptcha).