**Владислав Ткачик, Ірина Терещук**

**(Пирятин, Україна)**

**БЕЗПЕКА ВЕБ-САЙТА - ЗАХИСТ ВІД СПАМ РОБОТІВ**

*Актуальність.* Тривалий час методи захисту інформації розроблялися тільки державними органами, а їхнє впровадження розглядалося як виключне право тієї або іншої держави. Проте, в останні роки, з розвитком комерційної і підприємницької діяльності збільшилося число спроб несанкціонованого доступу до конфіденційної інформації, а проблеми захисту інформації виявилися в центрі уваги багатьох вчених і спеціалістів із різноманітних країн.

Оскільки основний інформаційний обмін сьогодення оснований на інформаційній технології, то важливою умовою безпеки стає безпека в комп'ютерних мережах. Тому захист інформації - важливе і першочергове завдання при проектуванні веб-сайтів.

Програмні засоби - це спеціальні програми і програмні комплекси, призначені для захисту інформації в інформаційних системах, наприклад PGP -комп'ютерна програма, а також бібліотека функцій, що дозволяє виконувати операції шифрування та цифрового підпису інформації; модулі сервера Apache: mod\_security та mod\_rewrite; CrackLib - бібліотека для перевірки даних у РНР-сценаріях.

З засобів програмного забезпечення систем захисту необхідно особливо виділити програмні засоби, що реалізують механізми шифрування (криптографії), та генерації електронно-цифрового підпису, наприклад, PGP.

У загальному випадку в систему забезпечення захисту інформації можуть бути включені [3]:

1) служба таємності даних - може бути використана для захисту переданих даних від можливості проведення аналізу інтенсивності потоків даних між користувачами;

2) служба аутентифікації - призначена для підтвердження того, що в даний момент зв'язку користувач є дійсно тим користувачем, за якого він себе видає;

3) служба цілісності даних - забезпечує доказ цілісності даних у процесі їхньої передачі, тобто забезпечує захист переданих повідомлень від випадкових і навмисних впливів, спрямованих на зміну переданих повідомлень, затримку і знищення повідомлень;

4) служба керування доступом - забезпечує захист від несанкціонованого доступу до інформації, що утримується в віддалених банках даних, або від несанкціонованого використання мережі;

5) служба цілісності інформації - забезпечує доказ цілісності повідомлення, прийнятого від відповідного джерела і знаходиться на збереженні;

6) служба доставки - забезпечує захист від спроб зловмисника порушити зв'язок.

Найбільш поширені способи захисту, метою яких є дозволити обробляти форму з даними виключно «живій» людині, а не боту (бот - спеціальна програма, що виконує автоматично і за заданим розкладом певні дії, видаючи себе за користувача):

* способи захисту, що потребують дій від користувача;
* способи, що не потребують дій від користувача;
* реєстрація користувачів та модерація коментарів.

1. Способи захисту, що потребують дій від користувача. Система захисту від спам-ботів САРТСНА - «спотворені» символи (цифри, букви) на форумах, гостьових книгах, при реєстрації нових користувачів, відправці SMS через Internet, які потрібно розпізнати і ввести з клавіатури. САРТСНА - це комп'ютерний тест, який використовують для того, щоб визначити, ким є користувач Web-сайту: людиною чи комп'ютером [2].

2. Способи, що не потребують дій від користувача. Ці способи захисту є більш дружніми до відвідувача сайту, ніж різного роду САРТСНА і тому при їх застосуванні зручність в користуванні сайтом для відвідувача зростає. Система може як обмежувати кількість запитів, так і намагатись відрізнити людину від бота за непрямими ознаками в поведінці.

Головна відмінність бота-програми від людини - це підхід до Web-сторінки як до послідовності тексту і тегів, тоді як пересічна людина бачить кінцевий результат (візуальний образ) і код сторінки її мало цікавить. Більшість способів, які не потребують активних дій від користувача при відправленні Web-форми, базуються на тому, що середньостатистичний бот, на відміну від повноцінного браузера, не навчений інтерпретувати CSS, JavaScript, Flash, тощо. Розглянемо деякі способи, які не потребують втручання користувача:

* обмеження по частоті повідомлень. Суть методу: необхідно стежити, щоб з однієї і тієї ж IP-адреси не було більше ніж, наприклад, десять повідомлень в хвилину. Він має сенс тоді, коли примушувати користувача вирішувати САРТСНА не можна, а захист є необхідним. Обмеження кількості запитів з однієї IP-адреси - це доволі простий спосіб, малоефективний при достатній підготовленості зловмисника;
* блокування за часом завантаження форми. Захистом може бути блокування при обробці повідомлення на певний час, що пройшов між завантаженням форми і її відправкою - людині, на відміну від бота, потрібен якийсь час на введення даних (який, як правило, більший за 1-2 секунди);
* блокування повідомлень за ключовими словами. Фільтр працює так: до публікації не допускаються повідомлення, що мають в тексті непристойні слова, образливі, лайливі фрази, або шкідливий програмний код;
* зміна імен полів, які беруть участь в передаванні даних. Більшість спам-роботів шукають на сторінці поля із стандартними іменами, наприклад, «nаmе», «email», «mail» і тому подібне. Щоб доставити боту деяку незручність, краще називати поля нестандартно. Або можна, наприклад, поле «електронна пошта» назвати «nаmе», а «ім'я» - «email», з розрахунку на те, що бот прийме рішення про суть полів по атрибуту name тегу <input>;
* створення полів-приманок. Спам-бот шукає поля «nаmе», «email» і тому подібні. Створюємо приховане поле, не hidden, а, наприклад, приховане засобами CSS. Звичайний відвідувач не бачить це поле і природно не заповнює його. Спам-робот заповнить це поле. Форма повинна оброблятися тільки, якщо приховане нами поле буде порожнім. Серед полів-приманок звичайно мають бути поля, які б бачив користувач, але їм слід дати нестандартні імена;
* блокування повідомлень за розміром екрану. Даний спосіб захисту працює за простою схемою: якщо при програмному визначенні у відвідувача нема розмірів (ширини, висоти) екрана, то форму намагається надіслати бот, отже її не слід обробляти;
* побудова форми за допомогою JavaScript. Цей метод робить аналіз форми ще складнішим: боту необхідно знайти і виконати код JavaScript, щоб отримати поле, яке слід заповнити. Можна, наприклад, заховати поле в JavaScript-код так [2]:

<form action="..." name="addMsg" method="post">

<script language="JavaScript" type="text/]avascript">

...

doсument.write('<inp'+'ut n'+'ame="a'+'ntis" t'+'ype="hi'+'dden" va'+'lue="1'+'10'+'4">');

...

</script>

</form>

А тоді на стороні сервера слід перевіряти чи існує $\_POST['antis'] та, чи вона дорівнює 1104.

3. Реєстрація користувачів та модерація коментарів. Суть цього методу полягає в тому, що, наприклад, коментарі в Гостьовій можуть залишати не всі відвідувачі, а лише ті, що зареєстровані на сайті. Реєстрація є бар'єром для масової розсипки спаму. Модерація коментарів полягає в тому, що публікуються тільки ті думки відвідувачів, що прямо схвалені адміністратором Web-pecypcy. [1].

Таким чином, в даній роботі розглянуті найбільш популярні засоби захисту сайту від атак спам-програм. Описані в ній приклади не гарантують на 100% від того, що сайт ніхто не «зламає» або не зашкодить йому. Завжди, навіть в популярних і довершених системах є вузькі місця, приклад тому випадок, коли на сайтах по всьому світу була знайдена груба помилка, яка дозволяла виконувати довільні запити до бази даних мовою SQL (Structured Query Language - структурована мова запитів). У подальшому шляхом розвитку та популяризації програмного забезпечення дані проблеми будуть зведені до мінімуму. Але і шкідливі програми будуть розвиватися тому дана проблема буде зажди актуальною.

**Література:**

1. Капча [Електронний ресурс] – Режим доступу до ресурсу: http://ru.wikipedia.org/wiki/CAPTCHA.
2. Полещук Я. Защита web- сервисов от спама [Електронний ресурс] / Ярослав Полещук. – 2007. – Режим доступу до ресурсу: http://captcha.opti-mail.net/.
3. Спецвыпуск журнала « Хакер ». // Гейм Лэнд. – 2007. – №75.

**Науковий керівник:**

викладач Терещук Ірина Вікторівна.