УДК 004.056

Н. В. Касянчук
А. А. Шиян

ОСОБЛИВОСТІ ЗАХИСТУ ВЕБ-САЙТІВ В РАМКАХ ЕЛЕКТРОННОГО УПРАВЛІННЯ

Вінницький національний технічний університет

Анотація

В ході дослідження було здійснено огляд особливостей захисту веб-сайтів та проведено аналіз моделей дискреційного розмежування доступом до інформаційних систем. Виявлено низку характерних особливостей, переваг і недоліків існуючих дискреційних моделей управління доступом.

Ключові слова: захист веб-сайтів, розмежування доступу, дискреційна модель.

Abstract

In the course of the study, an overview of the features of the protection of websites and an analysis of the models of discretionary division of access to information systems was conducted. A number of characteristic features, advantages and disadvantages of existing discretionary access control models are revealed.

Key words: website protection, access differentiation, discretionary model.

Вступ

Бурхливий розвиток інформаційних технологій призвів до інформаційної революції, внаслідок чого основною цінністю для суспільства взагалі й окремої людини зокрема поступово стають інформаційні ресурси. За таких обставин забезпечення інформаційної безпеки поступово виходить на перший план. Проблема розмежування доступу до даних стала центральним елементом систем безпеки комп'ютерної інформації.

Один із методів захисту інформації є система розмежування прав доступу до неї. Системи розмежування прав доступу здійснюють контроль за доступом суб’єктів інформаційної системи до об’єктів цієї системи. В основі будь-якої такої системи лежить модель розмежування прав доступу.

Метою даної роботи є аналіз моделей дискреційного розмежування доступу та розгляд особливостей захисту веб-сайтів.

Результати досліджень

На сьогоднішній день, майже всі брандмауери веб-ресурсів покликані захистити від основних типів загроз. А саме:

– SQL ін'єкція;
– міжсайтовий скриптинг (XSS);
– міжсайтова підробки запитів (CSRF);
– розподілена відмова в обслуговуванні (DDoS-атаки);
– відсутність таймаута сесії;
– зворотний шлях в директоріях.

Захист веб-сайтів від несанкціонованого доступу призначений для криптографічного захисту та розмежування доступу до інформації, оброблюваної в ІС, побудованих на базі Web-технологій.

При цьому забезпечується:

– взаємна автентифікація (підтвердження справжності) клієнта та сервера за протоколом, побудованим із використанням несиметричних криптографічних алгоритмів;

– захист конфіденційності та цілісності інформації, що передається між клієнтом та сервером, з використанням алгоритмів симетричного шифрування / дешифрування інформації та вироблення/перевіряння кодів автентифікації повідомлень;

– розмежування доступу користувачів до інформаційних ресурсів, представлених у вигляді статичних або динамічних Web-сторінок, що зберігаються та оброблюються на відповідних Web-серверах та потребують захисту (захищених Web-ресурсів).

Враховуючи усі особливості функціонування веб-сайтів та їх захист, постає проблема несанкціонованого доступу до інформації з боку осіб, котрі не мають дозволу на доступ до цієї інформації, та осіб, що мають право на доступ до цієї інформації в обсязі, що перевищує необхідний для виконання службових обов'язків.

Було визначено, що одним із найбільш перспективних методів захисту веб-сайтів є використання дискреційних моделей розмежування доступу.

Дискреційна модель розмежування доступу передбачає, що права доступу суб'єктів до кожного окремого об'єкта системи можуть бути довільним чином обмежені на основі деякого зовнішнього по відношенню до системи правила. Також дискреційна модель вимагає ідентифікованості всіх суб'єктів та об'єктів системи. [1]

Основним елементом дискреційного розмежування доступу є матриця доступу. Матриця доступу – це матриця D розміром |S|x|O|, рядки якої відповідають суб'єктам, а стовпчики – об'єктам. Кожний елемент матриці доступу D [s,o] ⊆ R визначає права доступу суб'єкта s до об'єкта o, де R – множина можливих прав доступу. [2]

Суб'єкти s - є активними сутностями, здебільшого це користувачі або процеси. Об'єкти o - є пасивними сутностями, що потребують захисту. Це можуть бути, наприклад, файли, записи баз даних, сегменти оперативної пам'яті. У деяких операціях доступу суб'єкти можуть виступати як пасивні сутності, до яких здійснюють доступ інші суб'єкти, тому множини S та O знаходяться у відповідності S ⊆ O.

У матриці доступу D кожен рядок відповідає певному суб'єктові s, а кожен стовпчик – об'єктові o. Елементом матриці D[s,o] є множина прав доступу, або повноважень суб'єкта s стосовно об'єкта o. Ці права, власне, і визначають, що може робити суб'єкт з об'єктом.

Проведений аналіз систем дискреційного розмежування доступу показав пріоритетність двох напрямів цього виду моделювання, а саме: матричного (модель Харрісона – Руззо – Ульмана) і потокового (класична модель Take – Grant, розширена модель Take – Grant).

Модель Харрісона – Руззо – Ульмана передбачає представлення системи розмежування прав доступу скінченним автоматом, який функціонує згідно з визначеними правилами переходу.[4-5]

Модель Take – Grant застосовується для аналізу систем дискреційного розмежування доступу. За допомогою чого підтверджується або спростовується ступінь захищеності даної інформаційної системи, яка повинна задовольняти регламентованим вимогам. Модель представляє всю систему як спрямований граф, де вузли графа – це, або об'єкти, або суб'єкти. Дуги між ними марковані, і їх значення вказують права, які має об'єкт чи суб'єкт.[6]

Вирішення задачі розмежування доступу в даних моделях зводиться до розв'язання оптимізаційної задачі на матриці або графі.

Висновки

Отже, в ході дослідження було розглянуто особливості захисту веб-сайті та визначено, що одним із найбільш перспективних методів захисту веб-сайтів є використання дискреційних моделей розмежування доступу, а саме моделі Харрісона – Руззо – Ульмана та Take – Grant. Також було виявлено основні переваги та недоліки даних моделей.

Основною перевагою дискреційної системи розмежування доступу є її проста реалізація і, як наслідок, її широка розповсюдженість на практиці.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Девянин П. Н. Модели безопасности компьютерных систем / П. Н. Девянин. – М. : Издательский центр "Академия", 2005. – 144 с.

2. Семенов С.Г. Методика настройки параметров распределения доступа и защиты информации в компьютерных системах критического применения / С.Г. Семенов // Системи озброєння і військова техніка. – Х.: ХУ ПС. – 2012. – Вип. 4(32). – С. 153-158.

3. Семенов С.Г. Методы и средства распределения доступа и защиты данных в компьютеризированных информационных управляющих системах критического применения / С.Г. Семенов. – Х.:НТУ «ХПИ», 2013. – 360 с.

4. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. — Феникс, 2008. — С. 34—40. — 173 с. — ISBN 978-5-222-13164-0.

5. Harrison M., Ruzzo W., Ullman J. ESIGN: Protection in operating systems (англ.). — 1976. — Август (т. 19, № 8). — С. 461–471. — ISSN 0001-0782

6. Миронова В. Г. Реализация модели Take-Grant как представление систем разграничения прав доступа в помещениях / В. Г. Миронова, А. А. Шелупанов, Н. Т. Югов // Доклады ТУСУРа. – 2011. – № 2 (24). – С. 206 – 210.

Касянчук Наталія Володимирівна– студентка групи УБ-18м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: natali109788@gmail.com

Шиян Анатолій Антонович - канд. фіз.-мат. наук, професор кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: Anatoliy.a.shiyan@gmail.com

Kasianchuk Nataliia V. - student of UB-18m group, faculty of Management and Information Security, Vinnitsa National Technical University, Vinnitsa, e-mail: natali109788@gmail.com

Shiyan Anatoliy A. – PhD, Professor of Department of Management and Information Systems Security, Vinnytsia National Technical University, Vinnytsia, email : Anatoliy.a.shiyan@gmail.com