Коляка Андрій Володимирович
Національний авіаційний університет, Київ,Україна

Удосконалена система автентифікації та керування доступом до веб-додатків

Вступ Інтернет став невід'ємною частиною життя і мережею, що постійно розвивається і яка змінила вид діяльності багатьох людей та організацій. Багато установ були атаковані, що призвело до великих втрат. Мережі організації, що не знають або ігнорують ці проблеми піддають себе великому ризику бути атакованими зловмисниками. Захист інформації, основним завданням якого є запобігання порушенню функцій інформаційної безпеки, займає перше місце по актуальності з поставлених задач.

Актуальність роботи визначається тим, що проблеми пов'язані з розмежуванням доступу і аутентифікації користувачів є критичними і організація цих механізмів є необхідним для сучасних веб-додатків.

Постановка завдання - створення системи розмежування доступу для користувачів різних ролів та механізму аутентифікації, який би забезпечував двофакторний механізм перевірки.

Мета – дослідження сучасних методів аутентифікації та керування доступом та реалізація системи, яка поєднує надійність, безпеку та зручність для її користувачів при виконанні даних операцій.

Викладення матеріалу Для реалізації можливості обмеження або контролю доступу до інтернет-баз даних, окремих програмних продуктів чи технологічних, офісних приміщень тощо, сьогодні застосовуються системи захисту, які передбачають наявність процесів ідентифікації, аутентифікації та наступної авторизації користувачів. При цьому, під ідентифікацією розуміється процедура розпізнавання користувача в системі, як правило, за допомогою наперед визначеного ідентифікатора або іншої апріорної інформації про нього, яка

сприймається системою; під автентифікацією розуміють процедуру встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора; під авторизацією розуміють керування рівнями та засобами доступу до певного захищеного ресурсу [1]. Однак, ідентифікація та авторизація можуть давати помилково вірний результат доступу у випадку введення ідентифікатора третіми особами. Для унеможливлення цього застосовується процедура автентифікації користувача за певними його індивідуальними ознаками. Відповідно, важливим є вибір як таких індивідуальних ознак так і самої процедури аутентифікації. Захист веб-додатків від зловмисників залежить від технологій і компонентів, що використовуються при створенні веб-додатків, а також від можливих уразливостей цих компонентів.

Уразливості контролю доступу на рівні функцій можуть бути викликані недостатнім захистом чутливих оброблювачів запитів в додатку. Додаток може просто приховати доступ до чутливих дій, не може забезпечити достатню, щоб отримати певних дій або ненавмисно виставити дію через керований користувачем параметр запиту. Ці уразливості можуть бути набагато складнішими і бути результатом тонких крайніх випадків в базовій логіці програми [2].

Для підвищення безпеки на практиці використовують декілька чинників автентифікації відразу. Проте, при цьому важливо розуміти, що не всі комбінації декількох методів є багатофакторною аутентифікацією. У основі одного з найнадійніших на сьогодні методів багатофакторної автентифікації лежить застосування персональних апаратних пристроїв — токенів. Токени дозволяють генерувати і зберігати ключі шифрування, забезпечуючи тим самим строгу автентифікацію. Використання класичних «багаторазових» паролів є серйозною уразливістю при роботі з чужих комп'ютерів, наприклад в інтернет-кафе. Це підштовхнуло провідних виробників ринку автентифікації до створення апаратних генераторів одноразових паролів. Такі пристрої генерують черговий пароль або за розкладом (наприклад, кожні 30 секунд), або за запитом (при натисненні на кнопку).

Кожен такий пароль можна використовувати тільки один раз. Перевірку правильності введеного значення на стороні сервера перевіряє спеціальний сервер автентифікації, що обчислює поточне значення одноразового пароля програмно. Для збереження принципу двохфакторності автентифікації окрім згенерованого пристроєм значення користувач вводить постійний пароль [3].

Висновки В даній роботі розглянуто можливі уразливості системи при аутентифікації та надання доступу різним типам користувачів. В результаті аналізу було спроектовано систему в якій поєднано механізми SSO (Single sign-on) та двофакторної перевірки, що забезпечує безпеку та надійність процесу аутентифікації у веб-додатку. Розроблено форму реєстрації з можливим варіантом вибору функції безпеки для привілейованих користувачів (адмінів). Дана система забезпечує надійність та безпеку у використанні веб-додатку для користувачів різних прав доступу.

Література:

1. Moffett J. Security & Distributed Systems [Електронний ресурс] / Jonathan Moffett – http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.22.2312&rep=rep1&type=pdf.
2. Угрозы несанкционированного доступа [Електронний ресурс]. – 2008. – https://zakonbase.ru/content/part/1183301
3. Martin Fowler. Microservices [Електронний ресурс] — https://martinfowler.com/articles/microservices.html Дата доступу: 09.10.2018