Кухар О.О. Козлов Р.С.
студенти,
Національний авіаційний університет

БЕЗПЕКА ВЕБ-СЕРВЕРІВ, ЩО ПРАЦЮЮТЬ НА ПЛАТФОРМІ ASP.NET

На сьогоднішній день, така платформа як ASP.NETпропонує послуги автентифікації та авторизації співпрацюючи з засобами типу IIS. Платформа підтримує у тому числі делегування прав клієнтів на рівнях запитів. Системи безпеки платформи ASP.NETна підставі ролі, яка була реалізована у аналогічних системах забезпечення безпеки типу COM+ дозволяє нам налаштовувати усю складову сторінки, виходячи з послідовного членства у деяких ролях. Та й взагалі такий вид додатку як ASP.NETможе у собі містити власний інтерфейс для реєстрації та виконання перевірок тої інформації, який може зникнути. Справді, такі підходи до даних проблем на багато разів спрощують процедури автентифікації, які застосовуються у сьогоденні на багатьох веб-сайтах [1].

У нашому житті трапляється чимало випадків, коли забезпечення безпеки – одна з останніх типів задач, які розглядають наші веб-розробники під час створення додатків такого плану. Дуже шкода, адже що стосується вимог безпеки, то ці важливі речі мають розглядатися більш детально аніж бажає цього веб програміст. Коли ми починаємо створювати такі типи додатків, то ставимо перед собою загальну мету: додаток має бути зручним та набагато комфортнішим у використанні. Але, коли аналізуєш усі типи вимог безпеки, розробник починає бачити, що у теперішній час потрібно розв’язувати абсолютно протилежні задачі.

Наразі що стосується створення безпеки, створює неабиякі проблеми той факт, що зв’язки, запити та багато інших видів комунікацій між веб – додатком та клієнтом виконується по дуже довгим конектам. І ось для вирішення питань, які пов’язані з безпекою веб- додатків потрібно використовувати автентифікацію. Попри цих речей клієнт має право знати відповіді на таке питання: Чи дійсно цей сайт створений компанією та оголошений у формі? Серверу завжди потрібна ідентифікація клієнта, (його потребують насамперед ті додатки, що мають дані, які турбують клієнта. (для прикладу банківський рахунок і.т.д.) [2].

Той рівень, який потрібно задати веб-розробнику залежить від суті створеного додатку. Бо трапляються і такі випадки, коли зведені дані про користувача можуть бути й непотрібними і багато з них будуть працювати з багатьма клієнтами, як з користувачами анонімного типу. А додатки, які видають лише спеціалізовану складову інформації, мають можливість проводити ідентифікацію клієнтів, якщо ті особи не мають ніяких заперечень з цього приводу, а що стосується анонімних клієнтів, то вони мають вільний доступ до цих ресурсів. Але все ж таки, додатки веб складової, які пропонують своїм клієнтам так звані спеціальні послуги (наприклад: дані біржі, банківських

рахунків, паспортних даних тощо). Мають потребу у автентифікації надійності клієнта перед тим як пропонувати таку сторінку сайту [3].

Якщо ми представляємо себе, як веб-розробники, ми повинні враховувати рівні автентифікації, якого потребує визначений додаток та додавати лише необхідні для нього засоби безпеки. Бо якщо у додатку таких засобів мало, то це може погрішити рівень зручності з точки зору праці з цим додатком [4].

Для клієнта дуже необхідно й важливо щоб такий сервер був аутентифікованим. Клієнт повинен мати високий рівень впевненості, що цей сайт, який він вирішив зненацька переглянути, створений веб-розробником, який працює у компанії та виконує його як вказане обличчя або організацією, у якій він обіймає свою посаду. Такі речі мають дуже велике значення, коли клієнт довіряє свої спеціальні дані серверу: номер паспорта або номер банківської картки. В іншому випадку якщо такий сервер не автентифіковує себе, то у клієнта не буде впевненості що він довіряє свої дані саме серверу а не злочинцю, який прикривається виглядом сервера, для того щоби прочитати спеціальні дані клієнта [5].

В мережах, які перебувають під постійним, а й іноді жорстким контролем – такі мають автентифікацію високого рівня. Визначений комп'ютер перевіряє на автентифікованість інформацію кожного введеного в нього повідомлення або надісланого запиту. У цих середовищах дуже гарно працюють протоколи безпеки під назвою Kerberos. Хоча при таких намаганнях розширити такі види технологій до Веб рівня, доводиться нерідко зіштовхуватись з так званими обмеження клієнтських брандмауерів, які унеможливлюють обмін секретними ключами безпечним [3].

Одне із багатьох вирішень даного питання стосується у використані так званих цифрових сертифікатів, у якого основа полягає у відкритому криптографічному ключі. Зазвичай на сервері зберігається закритий ключ а вже відкритий ключ публікується з метою того, щоб коли клієнти, використовувавши такий ключ, змогли ідентифікувати самий сервер. Хоча питання про зловмисника, який може будь-яким способом перехопити ключ який передається перевіреним сервером, замінивши його на особистий, залишається відкритим. Чому? Тому що після успішного завершення своїх брудних справ він матиме можливість перехоплювати, читати та модифікувати за власним розсудом будь-яку інформацію поміж клієнтом та сервером [4].

Але розв'язати такі виниклі проблеми можна за допомогою довіреної особи (його називають центром сертифікації), який засвідчує відкритий ключ як для клієнта так і для самого сервера. В якості прикладу наведемо компанію Verisign, яка змогла розгорнути свій унікальний центр сертифікації і за плату, яка визначена цією компанією, реєструє у себе відкритий ключ для кожного свого клієнта і зберігає у себе на сайті сертифікації та передає їх кожному бажаючому клієнту, засвідчуючи цим, що даний відкритий ключ дійсно належить особі, яка його зареєструвала. Якщо такому центру сертифікації можна давати довіру та клієнт не лінуватиметься перевіряти його використовуючи відкритий ключ сервера, то така система відмінно виконує свої робочі функції та задачі. Але все ж таки залишається питання Чи справді

клієнт спілкується з центром сертифікації, а не з особою, що скоює кіберзлочини? Надійним рішенням таких проблем є налаштування відкритих ключових центрів сертифікації на комп'ютер клієнта разом з браузером.

Отже, ключовою задачею автентифікації є гарантування ідентичності самого сервера. У той час як автентифікація клієнта переслідує декілька цілей різного значення. Для деяких сайтів автентифікація потрібно для того щоби змінювати складову даної веб-сторінки в залежності від бажань клієнта (як приклад деякі сайти виводять початкові сторінки, орієнтуючись на бажання свого клієнта). В сайтах, які мають інші напрями в залежності від ідентичності клієнта налаштовується різний доступ до різних частин інформації даного сервера. І нарешті, що стосується самого доступу до деяких сайтів, то клієнт повинен мати обліковий запис у тому сервері, яким він користуватиметься; до речі, щодо операцій клієнта посередньо веб-сайту, то такі можуть виконуватися лише за умов та основ облікової інформації клієнта (такі методи доступні у додатках intranet. Кожен з таких типів забезпечує свій рівень безпеки та може бути реалізований багатьма способами [2].

На самому ж сервері типу IISможна задавати різні типи рівнів ідентифікацій клієнтів для даних веб-додатків (або для сторінок даного додатка). За замовчуванням сервер IIS не має процедури автентифікації клієнтів, оскільки додаткові операції такого сервера над кожним клієнтом можуть знизити ефективність виробництва. Якщо ніяка автентифікація клієнта не задана, то кожен запит опрацьовується під виглядом анонімності з обліковим записом (IUSR_MACHINE, де MACHINE – ім'я комп'ютера). Для того щоби задати за допомогою IISавтентифікацію клієнта, потрібно вимкнути режим анонімного доступу та вибрати метод так званої автентифікації.

У діалоговому вікні сервера IISможна задавати режим базової автентифікації або інтегрованої автентифікації або дайджест-автентифікації. Процедура базової автентифікації вимагає від клієнта передачі пароля у вигляді звичайного підтексту. Взагалі базову автентифікацію використовують зазвичай тоді, якщо сайт використовує протокол захищених сокетів. (SSL – SecureSocetLayer).Але навіть якщо пароль вважається таким, що зашифрований, сценаріям веб-додатків та внутрішній змінній типу AUTH_PASSWORDвін залишається доступним, що знижує рівень загальної безпеки [1].

У режимі інтегрованої автентифікації можуть використовуватися такі засоби, як засоби тої самої автентифікації операційної системи Windows. Дана ж процедура автентифікації Windows співпрацює з системою безпеки Kerberos або NTLM (NT LAN Manager – диспетчер локальної мережі NT) з таким розширенням як HTTP. Воно застосовується лише для клієнтів, які мають браузери типу IE, і які ще мають дійсний обліковий запис на сервері та не віддалених від самого сервера брандмауером або так званим проксі – сервером, тому що сам брандмауер забороняє Kerberos, а повідомлення типу NTLM не будуть проходити через проксі-сервер. Цей режим дуже часто використовується в мережах локального призначення intranet, хоча він мало корисний для серверів типу Internet [4].

У процедурі типу дайджест-автентифікації для перевірок паролів клієнтів використовують метод «виклик-відповідь». (зазвичай його називають рукостисканням). Такий пароль повинен мати доступ у даному сервері, відповідно до цього, сервер повинен виступати у якості контролера – домену серверної мережі. Єдиний недолік, який помічений у таких типах конфігурацій полягає у наступному: Якщо зловмисник отримає доступ та контроль над доменом – це може мати катастрофічні наслідки [2].

Список використаних джерел:

1. Храмцов П.Б., Брик С.А., Русак А.М., Сурин А.И. – Основы WEB-технологий. – М.: ИТУИТ.РУ, 2003. – 512 с.
2. Роджерс Д. – Программирование на Microsoft JScript.NET. «Вильямс», 2002. – 352 с.
3. Дунаев В.В. JavaScript. – СПб.: «Питер», 2003. – 394 с.
4. Старыгин А. XML: разработка Web-приложений. – СПб.: «БХВ-Петербург», 2003. – 585 с.
5. Троелсен Э. C# и платфома.NET. Библиотека программиста. – СПб.: «Питер», 2007. – 796 с.

Кухар О.О. Козлов Р.С.
студенти,
Національний авіаційний університет

ВИКОРИСТАННЯ ОДИНИЧНИХ КВАНТОВИХ СТАНІВ У РОЛІ ІНФОРМАЦІЙНОГО РЕСУРСУ

Якщо коротко звернутися до історії, то квантова теорія інформації розбивається на дві частини: це інформаційна та механічна теорія, які були створені на початку 20 століття.

Мета цих теорій дати можливість нам пізнавати про квантовомеханічні стани та вивчати їхні можливості виконувати функції переносу та обробки інформації. Цей новий вид науки був створений у 60 роках двадцятого століття під час масштабного розвитку обчислювальних машин як наслідок при частому зменшенні розмірів таких цікавих й складних апаратів з деяким часом прийде така необхідність проводити етапи використання одиничних квантвоих станів у ролі інформаційного ресурса. Поруч з цим схожа перспектива – це перші труднощі а найперше це посилений вплив квантового шуму, який вважався однозначно руйнівним фактором. Хоча при найбільш поглиблених дослідженнях, то можна дійти до висновку, що квантовий шум може давати природню допомогу у той час коли передається або обробляється така інформація [1].

Квантова теорія інформації працює з квантовими явищами, досліджує їх властивості або можливості та вивчає: які технології можна використовувати у повсякденному житті. Як результат зробився висновок, що під час використання квантових станів, така річ має можливість підняти швидкість