УДК 004.056

Ю. В. БАРИШЕВ, В. А. КАПЛУН

Вінницький національний технічний університет, м. Вінниця

МЕТОД АВТЕНТИФІКАЦІЇ ВІДДАЛЕНИХ КОРИСТУВАЧІВ ДЛЯ МЕРЕЖЕВИХ СЕРВІСІВ

Анотація: В даній статті представлено аналіз методів авторизації користувачів мережевих сервісів. Запропоновано метод захисту мережевих сервісів, який передбачає розробку правил політики інформаційної безпеки не лише для користувачів, але й для робочих станцій, з яких цим користувачам дозволяється отримувати доступ до конфіденційної інформації. Таким чином для отримання доступу до інформаційного ресурсу необхідна як успішна автентифікація користувача, так і успішна автентифікація робочої станції перед початком сеансів обміну даними. Крім того метод передбачає шифрування даних, що передаються, на ключі, який залежить від параметрів автентифікації та даних, надісланих протягом сеансу зв’язку.

Ключові слова: автентифікація, гешування, комп’ютерна мережа, пароль, параметри робочої станції.

Аннотация: В данной статье представлено анализ методов авторизации пользователей сетевых сервисов. Предложено метод защиты сетевых сервисов, который предполагает разработку правил политики информационной безопасности не только для пользователей, но и для рабочих станций, с которых этим пользователям позволяется получать доступ к конфиденциальной информации. Таким образом для получения доступа к информационному ресурсу необходима как успешная аутентификация пользователя, так и успешная аутентификация рабочей станции перед началом сеансов обмена данными. Кроме того метод предполагает шифрование передающихся данных на ключе, который зависит от параметров аутентификации и данных, пересланных во время сеанса связи.

Ключевые слова: аутентификация, хеширование, компьютерная сеть, пароль, параметры рабочей станции.

Abstract: Network services users authentication methods analyses are performed at the article. The network services protection method, which is supposed information protection rules development for both users and workstations, which usage for getting access to confidential data by users is permitted. Thereafter to get the access to an informational resource both the user authentication and the workstation authentication should be passed before information exchange begins. Moreover the method is supposed to implement transferred data encryption with usage of the key, that depends on authentication parameters and data, which is transferred during the communication session.

Key words: authentication, hashing, computer network, password, workstation parameters.

Вступ

Комплексна природа процесу захисту інформації породжує необхідність аналізу багатьох загроз, які різні за своєю природою. І часто користь від використання потужних методів захисту інформації таких, як криптографічні методи, зводиться нанівець внаслідок впливу людського фактору [1]. Наприклад, використання протоколів автентифікації користувачів при обміні даними між ними та файловими серверами не може гарантувати захист конфіденційності інформації, що передається, на стороні отримувача цієї інформації, тобто користувача мережевого сервісу. Водночас використання мережевих сервісів дозволяє підприємцям пришвидшити обробку інформації. Останнє набуває особливої актуальності для підприємств, підрозділи яких територіально розподілені, однак потребують постійної взаємодії під час виробничого процесу. У зв’язку з тим, що витік інформації може відбуватися внаслідок візуального зняття інформації з моніторів комп’ютерів, фізичного втручання зловмисників в роботу працівників підприємства, які мають права на обробку конфіденційної інформації, тому важливо в політиці інформаційної безпеки обмежувати і способи обробки інформації, і робочі місця, з яких вона може бути здійснена. Саме тому актуальною є розробка методу комплексного захисту конфіденційності інформації для користувачів мережевих сервісів, який би дозволяв обмежувати доступ авторизованих користувачів до даних, якщо він відбувається з незахищених робочих місць.

Мета досліджень

Виходячи з вищенаведеного, метою даного дослідження визначено покращення захисту конфіденційності інформації, що надається мережевими сервісами, шляхом розробки методу та програмного засобу авторизації користувачів, який дозволить обмежити кількість робочих станцій, з яких можна здійснити авторизацію, та шифрувати дані, що передаються між робочою станцією та сервером.

Завдання досліджень

Для досягнення мети необхідно розв’язати такі задачі:

- проаналізувати відомі методи автентифікації користувачів;
- розробити метод автентифікації на основі гешування та прив’язки до параметрів робочої станції;
- розробити метод шифрування даних, що передаються;
- реалізувати дані методи у вигляді програмного засобу.

Аналіз відомих методів авторизації користувачів мережевих сервісів

Один з найбільш розповсюджених методів забезпечення авторизації користувачів у комп’ютерних системах базується на використанні ними пароля, що належить лише одному користувачу [2-4]. Під час автентифікації користувач вводить свій ідентифікатор і пароль. Еталонна пара логін-пароль зберігається в спеціальній базі [2, 5]. Процедура автентифікації в цьому випадку передбачає такі етапи [2, 4, 5]:

- користувач запитує доступ до системи і вводить особистий ідентифікатор та пароль;
- введені унікальні дані надходять на сервер, де порівнюються з еталонними;

- у випадку збігу даних з еталонними, автентифікація визнається успішною, при відмінності – користувачу пропонується знову ввести ідентифікатор та пароль.

Введений користувачем пароль може передаватися мережею таким чином [4-6]:

- у незашифрованому вигляді, на основі протоколу парольного автентифікації;
- з використанням шифрування;
- з використанням гешування.

В останніх двох випадках дані, що вводились користувачем, передаються мережею у захищеному вигляді. З точки зору максимізації захищеності, при зберіганні й передаванні паролів доцільніше використовувати гешування. Це пояснюється тим, що, перехопивши зашифрований пароль, зловмисник може зробити висновок про його довжину, що спростить йому реалізацію атаки підбору пароля. Крім того шифрування даних невеликої довжини (1-3 блоки даних) вразливе до атак збільшення довжини повідомлення – паддінгу (padding) [7] . Водночас геш-значення, отримане внаслідок виконання процесу гешування, завжди має сталу довжину незалежно від довжини вхідних даних гешування, в даному випадку – пароля, а тому не може бути об'єктом таких атак [3, 6, 8]. Саме тому більш стійкими до атак є методи, що передбачають зберігання на стороні сервера саме геш-значення пароля.

На рис. 1 наведено схему авторизації користувачів, що використовує збереження паролів у вигляді їх геш-значень [2, 5].

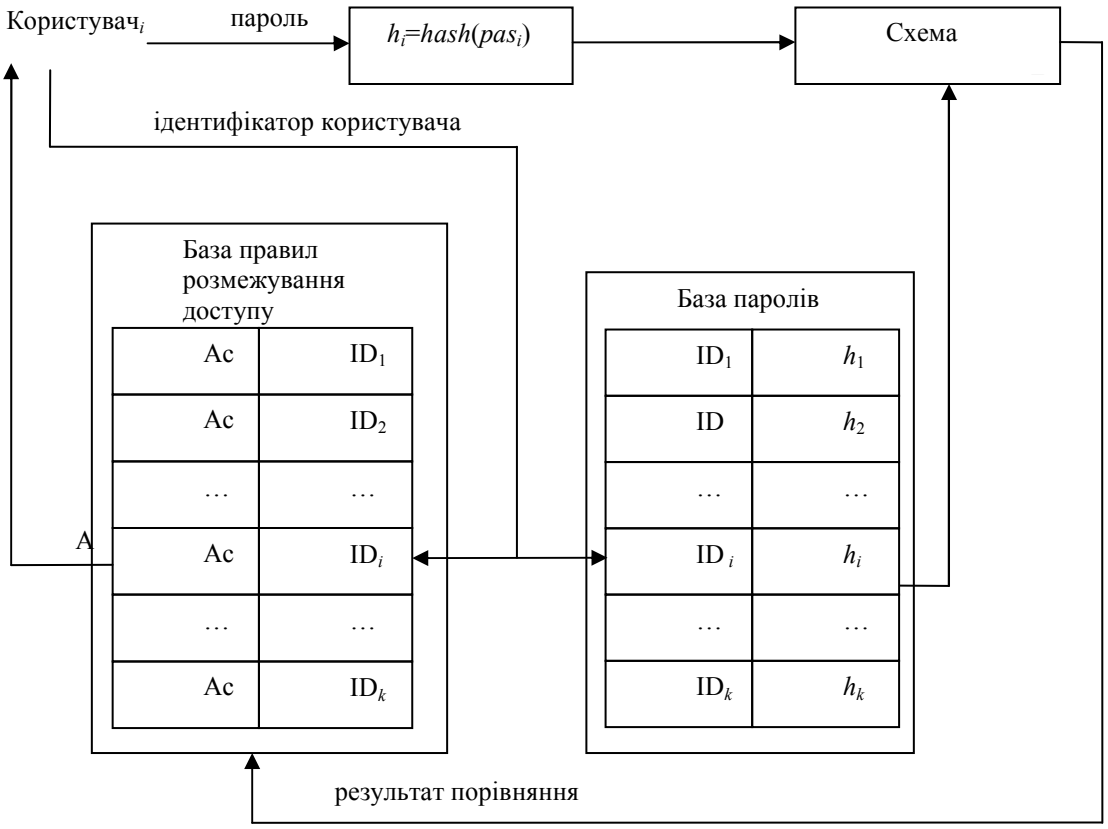

Рисунок 1 – Схема авторизації користувача з використанням паролів

де h_i – геш-значення пароля *i*-го кристувача; Access$_i$ – набір прав доступу для *i*-го кристувача; $hash(\cdot)$ – функція гешування;

З рис. 1 видно, що пароль використовуватиметься користувачем і при наступній авторизації, тобто він є багаторазовим. Використання багаторазових паролів має низку недоліків. По-перше, сам пароль, або його геш-значення зберігаються на сервері. Відповідно, отримавши доступ до них, зловмисник може, надсилаючи їх на сервер, імітувати користувачів та здобувати їх права доступу. По-друге, часто суб'єкт повинен запам'ятовувати пароль, тому розв'язання задачі вибору стійкого паролю покладається на нього. В такому випадку правильність розв'язання цієї задачі адміністратору з інформаційної безпеки складно перевірити, а зловмисник може отримати пароль, застосувавши навички соціальної інженерії [1, 2, 9].

При захисті програм від несанкціонованого копіювання, тобто автентифікації комп’ютерних систем, застосовуються методи, які передбачають внесення до програмного коду блоків, які впливатимуть на процес виконання програми залежно від параметрів комп’ютерної системи, на якій виконується даний код. Зазвичай дані блоки коду виконують перевірку автентичності комп’ютерної системи шляхом порівняння її поточних характеристик з еталонними [8, 9].

Методи автентифікації комп’ютерних систем попри схожість їх загальних алгоритмів, відрізняються параметрами комп’ютерної системи, за якими відбувається автентифікації цієї системи. Прив’язка відбувається на основі таких характеристик комп’ютерної системи [8, 9]: серійний номер жорсткого диску; дата створення та контрольна сума BIOS; версії та властивості операційних систем; вміст системних файлів; продуктивність апаратури; наявність додаткових пристроїв тощо. В певних випадках для надання унікальності кожному з сеансів автентифікації використовується криптографічна сіль [10].

Отже, процедури автентифікації комп’ютерної системи та її користувачів у відомих методах відбуваються незалежно одне від одного. Для протидії цьому використовуються криптографічні алгоритми, зокрема гешування та шифрування [2, 3, 6]. Шифрування даних, що передаються, в мережевих сервісах відбувається за алгоритмами симетричного або асиметричного шифрування [2, 3, 6]. Однак зашифровані дані автентифікації матимуть довжину, яка залежить від довжини вхідних даних. Саме тому доцільніше використовувати гешування, оскільки воно передбачає отримання вихідного значення фіксованої довжини незалежно від довжини вхідних даних.

Відомі методи автентифікації користувачів передбачають, що успішно авторизований, користувач не буде виконувати обробку інформації із застосуванням незахищеної робочої станції. З урахуванням, що причиною інцидентів у галузі інформаційної безпеки в переважній більшості випадків є людський фактор [1, 11] такі міркування – занадто оптимістичні, а тому не можуть мати місце при розробці розподілених інформаційних систем, в яких обробляється інформація цінна не лише для користувачів цієї системи.

Метод організації захищеного зв’язку користувачів

З розглянутого вище випливає, що при реалізації доступу до віддалених сервісів автентифікація користувача та системи, з якої відбувається спроба доступу повинна відбуватись одночасно, адже в цьому випадку адміністратор системи захисту інформації може переконатися в захищеності процесів обробки інформації на робочих станціях та заблокувати шляхи витоку інформації з них. Для цього авторами пропонується метод організації захищеного доступу користувачів до мережевих сервісів, який передбачає такі дії:

1. Введення ідентифікатора користувача до робочої станції.
2. Пересилання ідентифікатора користувача та ідентифікатора робочої станції до сервера.
3. Обчислення геш-значення на стороні робочої станції:

$$h_{ij} = f\left(h_0,\, pas_i \,||\, params_j\right),$$

де pas_i – пароль і-го користувача $\left(i = \overline{1,\, k}\right)$ мережі;

$params_j$ – параметри j-ї робочої $\left(j = \overline{1,\, n}\right)$ станції;

$f\left(\cdot\right)$ – функція гешування.

4. Надсилання отриманого геш-значення від робочої станції до сервера та його порівняння зі значенням, що зберігається на сервері.

5. Якщо геш-значення збігаються, то сервер надає користувачеві відповідні права доступу до мережевого сервісу, інакше зв’язок розривається.

6. Обмін між сервером і робочою станцією конфіденційними даними відбувається у зашифрованому вигляді, причому при першому сеансі обміну даними, як ключ шифрування використовується геш-значення пароля користувача h_i, що формалізується так:

$$data_1^* = E_{h_i}\left(data_1\right).$$

Очевидно, що при цьому розшифрування відбувається на тому ж ключі. Це можливо внаслідок того, що і авторизована сторона, і сервер при коректному завершенні кроку 5 мають підтвердження того, що пароль був введений користувачем правильно.

7. Кожен наступний сеанс обміну інформацією буде зашифровуватися з використанням ключа, який визначається шляхом гешування даних, пересланих під час попереднього сеансу обміну даними:

$$h_i^{(w)} = f\left(h_i^{(w)},\, data_{w-1}\right),$$

де $h_i^{(0)} = h_i$.

Відповідно розшифрування під час w-го сеансу обміну даними між сервером та робочою станцією пропонується виконувати відповідно до такої формули:

$$data = D_{h_i}\left(data^*\right).$$

На рис. 2 зображено схему авторизації користувача і робочої станції, що пропонується у даному методі. Вигляд бази даних автентифікації, наведеної на рис. 2, спрощено для більшої наочності методу.

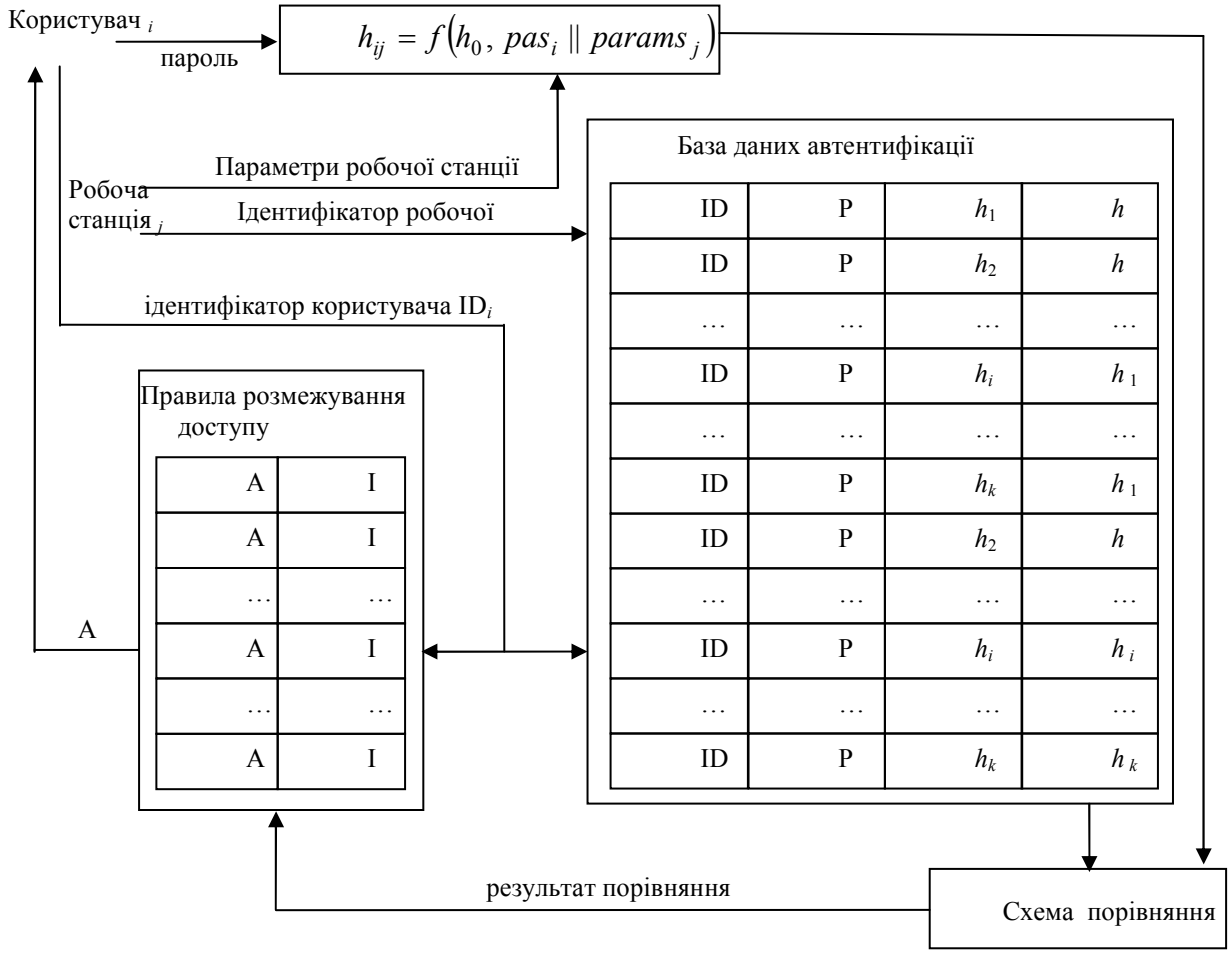

Рисунок 2 – Модифікована схема авторизації користувача з використанням паролів

З рис. 2 видно, що для успішної реалізації кроку 6 запропонованого методу в базі даних автентифікації передбачено наявність геш-значення пароля і-го користувача h_i, хоча власне під час автентифікації це геш-значення не використовується, а натомість використовується геш-значення h_{ij}.

Внаслідок впровадження методу кількість даних, якими обмінюються сторони під час авторизації, фактично не змінюється, оскільки ідентифікатор робочої станції повідомляється серверу ще на етапі створення зв'язку між ним та робочою станцією, відповідно в переважній більшості випадків ідентифікатор робочої станції буде відомим серверу ще до початку застосування методу. Відповідно в цих випадках автори пропонують спростити крок 2 методу та не пересилати ідентифікатор робочої станції. Дана модифікація дозволить не лише заощадити ресурси каналів зв'язку, але й ускладнити зловмиснику злам у випадку, коли він має можливість спостерігати за даними, що передаються між сторонами. У випадках, коли ідентифікатор робочої станції необхідно буде пересилати, кількість даних, що передаються також зросте незначно, оскільки для надання чотирьом мільярдам робочих станцій унікальних ідентифікаторів достатньо чотирьох байтів.

Висновки

Описаний вище метод дозволяє приховати від користувачів та від зловмисника, який відслідковує дані, які передаються, спосіб захисту, тим самим ускладнивши свій злам. З метою уникнення атак, пов’язаних із соціальним інжинірингом та візуальним зняттям інформації, запропонований метод, крім автентифікації користувача, передбачає автентифікацію робочої станції за її унікальними параметрами. Перевагою даного методу є те, що розмежування прав доступу користувачів відбувається не лише організаційними засобами, які можна обійти, але й криптографічними, на злам яких зловмисникам необхідно буде витратити набагато більше часу.

Список літератури

1. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире / Брюс Шнайер. – СПб.: Питер, 2003. – 368 с.

2. Защита информации в телекоммуникационных системах / Г. Ф. Конахович, В. П. Климчук, С. М. Паук, В. Г. Потапов. – К.: "МК-Пресс", 2005. – 288 с.

3. Информационная безопасность открытых систем: Учебник для вузов. В 2-х томах. Том 2. – Средства защиты в сетях / С. В. Запечников, Н. Г. Милославская, А. И. Толстой, Д. В. Ушаков. – М. : Горячая линия-Телеком, 2008. – 558 с.

4. Гайворонський М. В. Безпека інформаційно-комунікаційних систем. / М. В. Гайворонський, О. М. Новіков. – К. : Видавнича група BHV, 2009. – 608 с.

5. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.; Под ред. А. А. Шелупанова, С. Л. Груздева, Ю. С. Нахаева. – М. : Горячая линия-Телеком, 2009. – 552 с.

6. Петров А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. – М.: ДМК, 2000. – 448 с.

7. Vaudenay S. Security Flaws Induced by CBC Padding Applications to SSL, IPSEC, WTLS... / Serge Vaudenay. – 2002. – 12 p. – Режим доступу до статті: http://infoscience.epfl.ch/record/52417/files/IC_TECH_REPORT_200150.pdf

8. Дудатьєв А. В. Захист програмного забезпечення. Навчальний посібник. Частина 1. / А. В. Дудатьєв, В. А. Каплун, В. П. Семеренко. – Вінниця: ВНТУ, 2005. – 140 с.

9. Казарин О. В. Теория и практика защиты программ. / О. В. Казарин – М.: МГУЛ, 2004. – 450 с.

10.Biham E. A Framework for Iterative Hash Functions: HAIFA. / Eli Biham, Orr Dunkelman // NIST second cryptographic hash workshop. – 2006. – 9 с. – Режим доступу до статті: http://csrc.nist.gov/groups/ST/hash/documents/ DUNKELMAN_NIST3.pdf

11.Просис К. Расследование компьютерных преступлений / Крис Просис, Кевин Мандиа. – М. : Лори, 2012 – 416 с.

Відомості про авторів

Баришев Юрій Володимирович – к. т. н., старший викладач кафедри захисту інформації Вінницького національного технічного університету, Хмельницьке шосе, 95, м. Вінниця, 21021, службовий телефон (0432) 598 380; e-mail: yuriy.baryshev@gmail.com.

Каплун Валентина Аполінаріївна – старший викладач кафедри захисту інформації Вінницького національного технічного університету, Хмельницьке шосе, 95, м. Вінниця, 21021, службовий телефон (0432) 598 380.