Метод авторизації віддалених користувачів

Баришев Ю. В.[1], Неуйміна К. В.[2]

[1] К. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, Україна, yuriy.baryshev@gmail.com

[2] Студентка, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, Україна, kris.vladimirovna99@gmail.com

Анотація — Поширення мобільних обчислювальних систем обумовило необхідність перегляду сучасних підходів до автентифікації користувачів. За результатами виконаного аналізу визначено, що найбільш поширений метод автентифікації на основі паролю може бути модифікований для мобільних обчислювальних систем. Запропоновано схему авторизації користувача, що передбачає його прив'язку до обчислювальних систем.

Ключові слова: автентифікація, авторизація, пароль, прив'язка.

Remote user authorization method

Baryshev Y.V.[1], Neuimina K.V.[2]

1 PhD (ukr), Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Khmelnytske shosse 95,, Vinnytsia, Ukraine, yuriy.baryshev@gmail.com

2Student of Information Technologies and Computer Engineering Department, Vinnytsia National Technical University, Khmelnytske shosse 95, Vinnytsia, Ukraine, kris.vladimirovna99@gmail.com

Abstract — The necessity of the modern user authentication approaches revision was caused by mobile computer systems spreading. It was determined basing on the performed analyses results, that the most common method based on the password could be modified for mobile computer systems. The user authorization scheme was proposed, which requires his bounding with computer systems.

Key words: authentication, authorization, password, bounding.

Вступ

Більшість сучасних методів автентифікації користувачів передбачають використання паролю [1-4]. Перевагою даного методу є те, що він є простим як у реалізації, так й у використанні. Кожний користувач сучасних інформаційно-комунікаційних систем декілька разів на день приймає участь у процедурах ідентифікації та автентифікації. Процес парольної автентифікації не вимагає додаткових витрат: він реалізований у більшості програмних продуктів. Таким чином, система захисту інформації виявляється простою і доступною. Однак мобільні обчислювальні системи сприяють тому, що авторизовані користувачі отримують доступ до конфіденційної інформації за допомогою засобів, які не пристосовані для забезпечення відповідного рівня захищеності для цих даних [5].

Метою даних досліджень є покращення методів авторизації користувачів на сонові паролю шляхом розпізнавання комп'ютерних систем, призначених для проведення процедури авторизації.

Для досягнення мети необхідно виконати аналіз вже існуючих методів автентифікації та авторизації користувачів.

Аналіз відомих методів автентифікації користувачів

Важливим елементом забезпечення цілісності конфіденційної інформації є захист від несанкціонованого доступу до ресурсів інформаційних систем, що викликає необхідність створення надійних і зручних систем контролю доступу [1-3, 6]. Кожен користувач сучасних інформаційно-комунікаційних систем декілька разів на день стикається з процедурами автентифікації та авторизації. Ці процедури виконуються кожний раз, коли користувач вводить пароль для доступу до інформаційної системи, мережі, бази даних або при запуску прикладної програми. В результаті їх виконання користувач або отримує доступ до певних ресурсів інформаційної системи, або не отримує.

Під час цього процесу відбувається ідентифікація користувача, тобто процедура розпізнавання користувача в системі за допомогою наперед визначеного імені (ідентифікатора) або іншої інформації про нього, яка сприймається системою [1, 3, 4]. Вона є початковою процедурою надання доступу до системи, після неї здійснюється автентифікація та авторизація.

Автентифікація передбачає перевірку належності ідентифікатора об'єкту, тобто встановлення чи підтвердження дійсності, і перевірка чи є об'єкт або суб'єкт, що перевіряється, справді тим, за кого він себе видає [3, 4].

Процедуру автентифікації віддаленого користувача в мережі можна представити наступним чином. При спробі входу в мережу користувач вводить ідентифікатор та дані, на основі яких він автентифікується. Ці дані надходять і за ідентифікатором користувача знаходиться відповідний еталонний запис даних автентифікації. Якщо вони збіглись з даними, отриманими від користувача, то автентифікація відбулась успішно — користувач отримує ті права та ресурси мережі, які визначені для його статусу в системні. Тобто користувач авторизується [2].

Таблиця 1 – Таблиця відповідностей ідентифікаторів користувачів

Ідентифікатор користувача	Еталонне значення	Пава доступу
ID_1	E_1	$Access_1$
ID_2	E_2	$Access_2$
…	…	...
ID_N	E_N	$Access_N$

Передавання даних автентифікації та ідентифікатора користувача може відбуватись декількома способами [1, 4, 7]:

- в незашифрованому вигляді; наприклад, згідно протоколу парольної автентифікації PAP (Password Authentication Protocol) паролі передаються лінією зв'язку у відкритій незахищеній формі;

- в захищеному вигляді; всі дані, що передаються (логін і пароль користувача, випадкове число і мітки часу) захищені за допомогою шифрування або однонаправленої функції.

Варіант автентифікації з передачею паролю користувача в незашифрованому вигляді не гарантує навіть мінімального рівня безпеки, так як він схильний до чисельних атак. Для захисту паролю, його необхідно зашифрувати перед пересиланням незахищеним каналом [6]. Для цього в схему автентифікації включають засоби шифрування E_K та розшифрування D_K, керовані розподіленим секретним ключем K. Перевірка автентичності користувача базується на порівнянні паролю E_K, який був відправлений користувачем і вихідного значення, який зберігається на сервері автентифікації [8].

Крім того, досить часто [1-4, 7, 8] замість шифрування використовується гешування даних, за якими відбувається авторизація користувача. Перевагою геш-значення над шифротекстом є сталість довжини, що запобігає створенню уявлення у зловмисника щодо обсягу даних, за якими відбувається автентифікація користувача.

Існує декілька методів автентифікації, які відрізняються своєю складністю, надійністю, вартістю та іншими показниками. В інформаційних технологіях використовуються такі види автентифікації [3, 6-8]:

на основі знання секрету, зокрема паролю;

на основі біометричних характеристик користувача;

на основі володіння спеціальними технічними засобами.

Жоден з цих підходів не дозволяє виключити можливість використання робочих станцій, непридатних для обробки конфіденційної інформації. У часи, коли не було портативних комп'ютерних систем такий підхід був виправданим. Однак, сьогодні, коли користувач має більше одного засобу для отримання даних він використовуватиме для авторизації той з них, який найбільш зручний для нього в конкретний момент часу, не враховуючи, що даний засіб не підтримує необхідний рівень захисту даних, що за його допомогою обробляються.

Метод прив'язки користувачів до робочих станцій

Пропонується метод, який під час автентифікації передбачає побудову процесу автентифікації на основі гешування значень секретних даних користувача та параметрів робочої станції.

На рис. 1 зображено схему авторизації користувача і робочої станції.

З рис. 1 видно, що в базі даних автентифікації передбачено наявність геш-значення пароля і-го користувача h_i (або будь-яких інших даних, що автентифікують користувача). Ітеративність процесу гешування [9] дозволяє на стороні сервера отримати геш-значення аналогічне геш-значення користувача навіть без знання його ключа. Така властивість цього процесу дозволяє уникнути необхідності зберігання ключів гешування на стороні сервера. Що, в свою чергу, запобігає компрометації інших користувачів системи, коли зловмисник зумів підібрати/викрасти ключ одного з користувачів або отримав доступ до бази.

Для ідентифікації робочої станції пропонується використовувати комбінацію з декількох унікальних параметрів цієї станції.

Прив'язка відбувається на основі таких характеристик комп'ютерної системи [10]:

- серійний номер жорсткого диску;

- дата створення та контрольна сума BIOS;

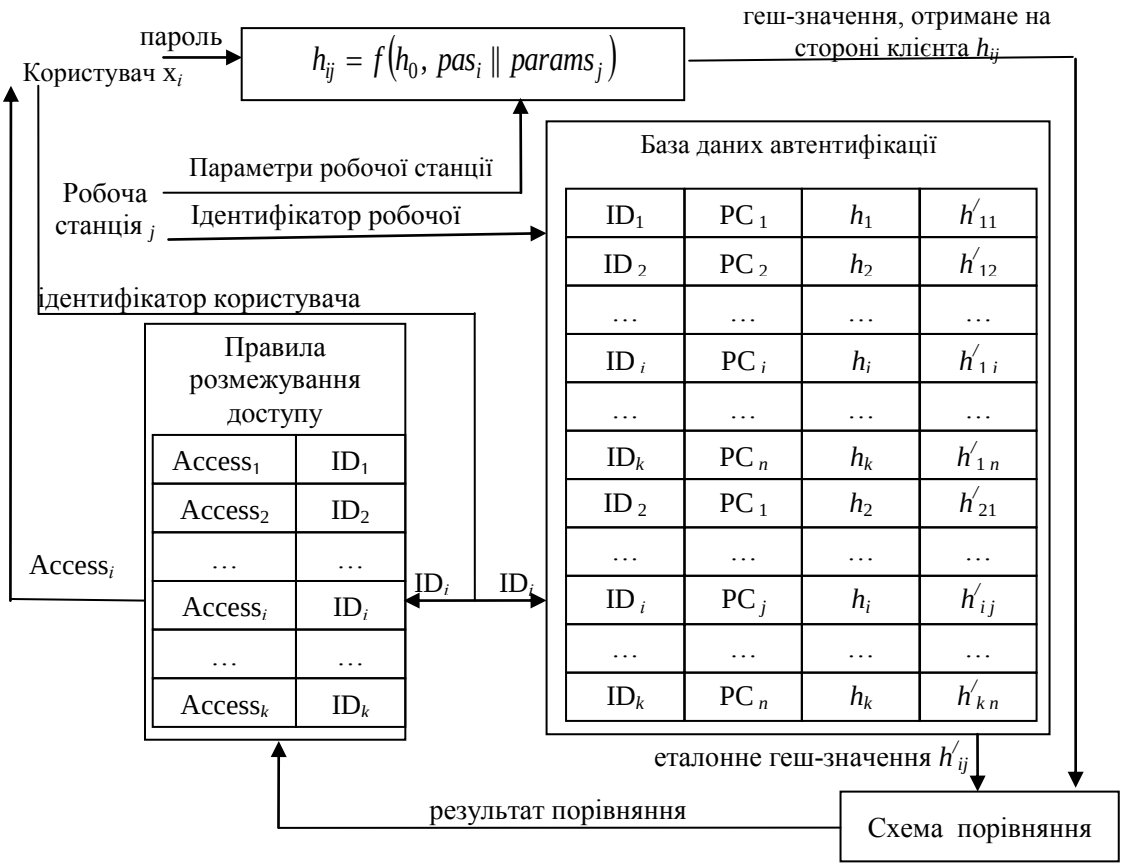

Рисунок 1 – Модифікована схема авторизації користувача з використанням паролів

- версії та властивості операційних систем;
- вміст системних файлів;
- продуктивність апаратури;
- наявність додаткових пристроїв тощо.

В певних випадках для надання унікальності кожному з сеансів автентифікації пропонується додавати криптографічна сіль – псевдовипидкові числа. Закон формування криптографічної солі для даного методу відомий на стороні сервера та клієнта.

ВИСНОВКИ

У дослідженні було проаналізовано відомі методи автентифікації. На основі аналізу сучасних методів автентифікації було виявлено, що відомі методи мають суттєвий недолік – вони не дозволяють обмежувати використання мобільних обчислювальних засобів для обробки конфіденційної інформації. Для усунення даного недоліку запропоновано схему авторизації та наведено перелік рекомендованих параметрів за якими можна виконати автентифікацію робочої станції. Недоліком запропонованого методу є ускладнення процесу адміністрування. Відповідно його доцільно використовувати в системах, де збитки від втрати інформації, що знаходиться на сервері перевищують зарплату додаткового системного адміністратора.

ЛІТЕРАТУРА REFERENCES

[1] Галатенко В. А. Основы информационной безопасности : учеб. пос. / В. А. Галатенко ; под ред. академика РАН В. Б. Бетелина. – 4-е изд. – М. : МГИУ, 2008. – 160 с.

[2] Методы аутентификации [Электронний ресурс]. – Режим доступа : http://www.panasenko.ru/Articles/69/

[3] Охота Д. Б. Технології комп'ютерної безпеки : монографія / Д. Б. Охота. – Рівне : МЕГУ, 2011. – 97 с.

[4] Романец Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин ; под ред. В. Ф. Шаньгина. – 2-е изд., перераб. и доп. – М. : Радио и связь, 2001. – 376 с.

[5] D. R. Thomas. Security Metrics for the Android Ecosystem. / Daniel R. Thomas, Andrew Rice // ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices – 2015. – Режим доступу до ресурсу : https://www.cl.cam.ac.uk/~drt24/papers/spsm-scoring.pdf

[6] Матвеев И. А. Распознавание человека по радужке / И. А. Матвеев, К. А. Ганькин // Системы безопасности. – 2004. – № 5. – С. 72–76.

[7] Сарбуков А. Аутентификация в компьютерных системах / А. Сарбуков, А. Грушо // Системы безопасности. – 2003. – № 5 (53). – С. 25–29.

[8] Шрамко В. Н. Защита компьютеров: электронные системы идентификации и аутентификации / В. Н. Шрамко // PC Week/RE. – 2004. – № 12. – С. 15–21.

[9] B. Preneel. Analysis and design of cryptographic hash functions. Katholieke Universiteit Leuven, 1993, p. 323 http://homes.esat.kuleuven.be/~preneel/phd_preneel_feb1993.pdf

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