УДК 004.056

К. В. Неуйміна
Науковий керівник: Ю. В .Баришев

МЕТОДИ АВТЕНТИФІКАЦІЇ ВІДДАЛЕНИХ КОРИСТУВАЧІВ

Анотація

Дослідження, присвячені розгляду та аналізу сучасних підходів, які використовуються сьогодні для автентифікації користувачів комп'ютерних систем. Визначено найбільш поширеним є метод автентифікації на основі паролю, проаналізовано його переваги та недоліки, запропоновано шляхи вдосконалення даного методу.

***Ключові слова**: автентифікація, ідентифікація, пароль, автентифікатор, USB-токен, смарт карта, електронний ключ, конфіденційність, інформаційна безпека.*

Abstract

The research is devoted to the review and analysis of modern approaches which are used today for authentication of users of the computer systems. The method of authentication based on a password was determined as the most common, it's advantages and disadvantages were analyzed and ways of its improving were proposed.

***Key words:** authentication, identification, password authenticator, USB-token, smart card, electronic key, privacy, information security.*

Одним з найбільш розповсюджених методів автентифікації є автентифікація користувача на основі паролю [1]. Перевагою даного методу є те, що він є простим як у реалізації, так й у використанні. Процес парольної автентифікації не вимагає додаткових витрат: він реалізований у більшості програмних продуктів. Таким чином, система захисту інформації виявляється простою і доступною.

Метою даних досліджень є покращення захисту конфіденційності інформації користувачів, шляхом встановлення надійного паролю.

Для досягнення мети насамперед необхідно виконати аналіз вже існуючих методів, які вже знайшли широке застосування. Суть парольної автентифікації полягає в тому, що кожен зареєстрований користувач певної системи одержує набір персональних реквізитів (зазвичай використаються пари логін-пароль) [3]. Далі при кожній спробі входу він повинен вказати свою інформацію. Оскільки вона унікальна для кожного користувача, то на підставі її система й робить висновок про особистість та ідентифікує її. Процедуру автентифікації користувача в мережі можна представити наступним чином. При спробі входу в мережу користувач набирає свої логін та пароль. Ці дані надходять і за логіном користувача знаходиться відповідний запис. З нього отримується пароль і порівнюється з тим паролем, який ввів користувач. Якщо вони збіглись, то автентифікація відбулась успішно — користувач отримує ті права та ресурси мережі, які визначені для його статусу системної авторизації. На рис. 1 зображено схему автентифікації на основі паролю [2].

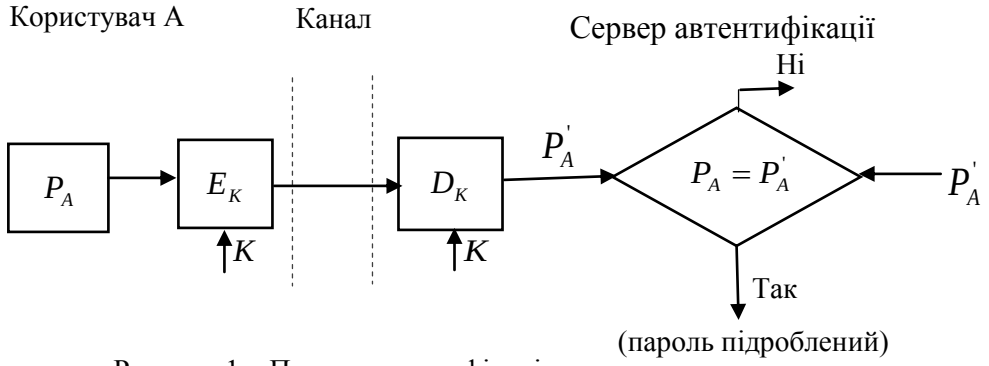

Рисунок 1 – Проста автентифікація з використанням паролю

Передача паролю та логіну користувача може відбуватись декількома способами [5]:

– в незашифрованому вигляді; наприклад, згідно протоколу парольної автентифіка-ції 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 [4]. 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. Якщо значення E_K і $P_A^{'}$ збігаються, то пароль P_A вважається автентичним, а користувач A — законним [6].

Крім того, необхідно щоб користувач міг здійснювати вхід лише з обмеженого кола комп'ютерів, відповідно запуск і робота додатків також має виконуватись не на кожному комп'ютері. Попри те, що існує безліч відомих методів автентифікації, які мають багато переваг, служба безпеки не гарантує повної захищеності секретної інформації. У зв'язку з цим необхідно встановити захист від несанкціонованого доступу шляхом прив'язки до флеш-носія.

Наприклад, якщо особа, знаходячись у громадському транспорті, вводить свій логін і пароль, то зловмисник може відслідкувати порядок їх введення. Отже, необхідно забезпечити надійний захист.

У дослідженні було проаналізовано відомі методи автентифікації. Досліджено основні проблеми методу на основі парольного захисту. Очевидні переваги парольної автентифікації – відсутність додаткових витрат, оскільки парольна автентифікація є складовою частиною всіх сучасних операційних систем. Найголовніший недолік парольної автентифікації – величезна залежність надійності автентифікації від самих користувачів, точніше, від обраних ними паролів. Також недоліком даного методу є те, що без використання інших механізмів захисту парольний захист, сам по собі, не є надійним, оскільки не може забезпечити потрібного захисту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

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. Задонский А. Ю. Вопросы аутентификации в современных информационных системах / А. Ю. Задонский [Электронный ресурс]. – Режим доступа : http://www.compserv.ru/
3. Методы аутентификации [Электронний ресурс]. – Режим доступа : http://www.panasenko.ru/Articles/69/
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. Сарбуков А. Аутентификация в компьютерных системах / А. Сарбуков, А. Грушо // Системы безопасности. – 2003. – № 5 (53). – С. 25–29.
6. Шрамко В. Н. Защита компьютеров: электронные системы идентификации и аутентификации / В. Н. Шрамко // PC Week/RE. – 2004. – № 12. – С. 15–21.

Відомості про авторів

Баришев Юрій Володимирович – к. т. н., доцент кафедри захисту інформації Вінницького національного технічного університету, Хмельницьке шосе, 95, м. Вінниця

Неуйміна Крістіна Володимирівна – студентка кафедри захисту інформації Вінницького національного технічного університету, Хмельницьке шосе, 95, м. Вінниця, e-mail: kris.vladimirovna99@gmail.com

Baryshev Yuriy Volodymyrovych – c.t.s, assistant professor of information security Vinnitsa National Technical University, Khmelnytsky Highway 95, m. Vinnytsya

Neuimina Kristina Volodymyrivna – student of the department of information security Vinnitsa National Technical University, Khmelnytsky Highway 95, m. Vinnytsya, e-mail: kris.vladimirovna99@gmail.com