УДК 004.056.53

О. В. Бондаренко

ЗАХИСТ ВІД НЕСАНКЦІОНОВАНОГО ЗАВОЛОДІННЯ ПАРОЛЕМ У СИСТЕМАХ БЕЗПЕКИ

Вінницький національний технічний університет

Анотація

В даній роботі досліджуються переваги та недоліки реалізації сучасних методів аутентифікації для захисту від несанкціонованого доступу в системах безпеки. Предметом дослідження є метод забезпечення інформаційної безпеки, заснований на аутентифікації користувача, за допомогою графічного пароля.

Ключові слова: аутентифікація, пароль, інформаційна безпека, парольна аутентифікація, біометрична аутентифікація, графічний пароль.

Abstract

This paper explores the advantages and disadvantages of implementing modern authentication methods to protect against unauthorized access to security systems. The subject of the study is a method of providing information security based on user authentication using a graphical password.

Keywords: authentication, password, information security, password authentication, biometric authentication, graphic password.

Вступ

В даний час існує велика кількість проблем в сфері інформаційної безпеки. Інформаційна безпека - це захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, що можуть призвести нанесенням шкоди власникам або користувачам інформації і підтримуючої інфраструктури. Однією з проблем в сфері інформаційної безпеки є проблема авторизації користувача та його аутентифікації.

Аутентифікація являє собою один із основних бар'єрів, що з'явилися в інформаційних системах та яка реалізовує множинний доступ до інформаційних ресурсів. Саме вона стоїть на першому етапі контролю. До основних переваг цієї методики захисту належать її простота та звичність. Значний відсоток інцидентів у сфері інформаційної безпеки трапляються внаслідок використання слабких паролів. Проводяться дослідження щодо визначення уразливості елементів в системах інформаційної безпеки. Результатом яких є підтвердження того, що найбільш вразливе місце в інформаційних системах – це слабкі паролі користувачів.

Саме тому виникає необхідність підвищення рівня інформаційної безпеки засобами вдосконалених методів аутентифікації.

Результати дослідження

Аутентифікація – процедура перевірки достовірності суб’єкта, яка дозволяє впевнитися в тому, що суб’єкт, пред’явивши свій ідентифікатор, дійсно є саме тим суб’єктом, ідентифікатор якого він використовує, тобто підтверджується відповідність суб’єкта ідентифікатору. Для цього користувач підтверджує факт про володіння деякою інформацією, яка доступна лише йому одному (пароль, ключ і тощо) [1].

Щоб захистити дані користувача, було запропоновано багато методів аутентифікації. На жаль, у кожного типу аутентифікації є свої переваги та недоліки. Жодна з методів аутентифікації не відповідає усім вимогам безпеки, а також потребам користувача. Введено різні процедури аутентифікації:

- аутентифікація на основі знань (буквено-цифрові паролі, графічні паролі);
- аутентифікація на основі маркера;
- аутентифікація на основі біометрії.

Одним із найпоширеніших методів захисту інформаційних систем на сьогоднішній день є парольний захист.

Основний принцип роботи даних систем полягає в ідентифікації й аутентифікація користувача шляхом запиту додаткових даних, якими можуть бути назва фірми і/або ім'я і прізвище користувача і його пароль або тільки пароль/реєстраційний код. Така інформація може запитуватися в різних ситуаціях, наприклад, при старті програми, після закінчення терміну безкоштовного використання ПЗ, при виклику процедури реєстрації або в процесі установки на ПК користувача.

Безпека в сучасних інформаційних системах залежить значною мірою від якості випадково обраних користувачем (Адміністратор) або згенерованих автоматично паролів.

Парольна політика включає в себе правила формату пароля, автоматичне блокування, політику зміни та відновлення пароля. Це ті вимоги яких рекомендується дотримуватись і які необхідні для підвищення стійкості парольного захисту [2].

Проблема суміщення легкості запам’ятовування, з одного боку, та високого рівня стійкості пароля до відтворення, з іншого, призвела до появи системи аутентифікації на основі графічних зображень. Психофізіологія людини така, що наш мозок здатен до зберігання великої кількості графічної інформації – в порівнянні з символьними паролями графічні легше і на більш довгий час запам’ятовуються, а тому з меншою ймовірністю потребують збереження їх на матеріальних носіях [4]. Але навіть записаний на матеріальному носії графічний пароль в окремих випадках досить складно інтерпретувати. Графічні дані в електронному вигляді являють мільйони байтів інформації і забезпечують великі можливості для унікальності вибору пароля.

На жаль, поширені підходи до введення паролів за допомогою клавіатури, миші, сенсорного екрана чи будь-якого традиційного пристрою введення, в основному, вразливі до таких атак, як атака «підглядання через плече» та атака з нанесенням пароля.

Застосування методу автентифікації на основі графічних паролів повинно забезпечувати захист введеної користувачем ключової інформації від витоку через прямий візуальний канал, тобто «підглядання через плече», від витоку інформації із застосуванням прихованих відеокамер та різних клавіатурних шпигунів. Скомпрометовані графічні паролі легко замінити, як і прості символьні, що є перевагою над біометричними даними.

В даний час об'єкти інформатизації використовують різні методи аутентифікації користувачів, одним з яких є метод аутентифікації за допомогою графічних паролів.

Графічні паролі є більш практичними для користувачів та за допомогою яких значно підвищується рівень інформаційної безпеки та захищеності даних. Підібрати графічний пароль за допомогою будь-якого словника нереально, тому що немає жодних доступних для пошуку словників для графічної інформації, а комп’ютеру для обробки мільйонів байтів інформації у процесі підбору варіантів графічного пароля необхідна значна кількість часу.

Отже, графічні системи паролів являють собою одну із перспективних альтернатив традиційним системам автентифікації на основі пароля.

Висновки

Застосування методу аутентифікації за допомогою графічних паролів, дозволяє забезпечити безпеку введеної користувачем ключової інформації. Враховуючи особливості різних методів аутентифікації, проведено аналіз, в результаті якого встановлено, що за допомогою графічної аутентифікації можливо забезпечити прийнятний захист системи від несанкціонованого заволодіння паролем. Вдосконалення методу графічної аутентифікації дозволить вирішити ряд проблем, які існують в сучасних системах аутентифікації користувачів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Термінологічний довідник з питань технічного захисту інформації: довідник / [С. Р. Коженевський, Г. В. Кузнецов, В. О. Хорошко, Д.В. Чирков]. – К.: ДУІКТ, 2007. – 365 с.

2. Єсін В.І. Безпека інформаційних систем і технологій / В. І. Єсін, О. О. Кузне-цов, Л. С. Сорока. – Харків: ХНУ імені В. Н. Каразіна, 2013. – 632 с.

3. Азарова А.О. Методичні вказівки до проведення практичних занять та до виконання самостійної індивідуальної роботи з дисципліни «Основи науково-дослідної роботи» для студентів напрямів підготовки 6.030601 – «Менеджмент» та 6.170103 – «Управління інформаційною безпекою» / Аза-рова А.О., Карпінець В.В. – Вінниця: ВНТУ, 2013. – 44 с.

4. Ананьєв О.М. Інформаційні системи і технології в комерційній діяльності / О.М. Ананьєв, В. М. Білик, Я. А. Гончарук. – Львів : Новий Світ-2000, 2006. - 584с.

Бондаренко Олександр Володимирович – студент групи УБ-19м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м.Вінниця, email: fm.ub15b.bondarenko@gmail.com

Науковий керівник: ***Карпінець Василь Васильович*** – к.т.н., доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця.

Bondarenko Oleksandr V. – student of UB-19m group, Department of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, email: fm.ub15b.bondarenko@gmail.com

Supervisor: ***Vasyl V Karpinets –*** Cand. Sci. (Eng.), Docent of Department of Management and Information Systems Protection, Vinnytsia National Technical University, Vinnytsia