МЕНЕДЖЕР ПАРОЛІВ ДЛЯ КІБЕР-ФІЗИЧНИХ ВИРОБНИЧИХ СИСТЕМ

Мамєдов А. А.
Науковий керівник – к.т.н., ст. викл. каф. КІТАМ Демська Н.П.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, кафедра КІТАМ)
тел. (057) 702-14-86
e-mail: andrii.mamiedov@nure.ua

In this work, with the aim of creation of the own comfortable manager of passwords, counted on storage of plenty of registration data and simultaneous work of plenty of users, actuality of problem is reasonable the most essential criteria are educed for his development.

Тенденції розвитку сучасного світу ведуть до збільшення обсягів інформації, підвищення вимог до її точності і своєчасного подання для аналізу і ухвалення рішень в режимах реального часу, тому вимагають перегляду підходів до використання високих технологій та їх ролі в різних сферах діяльності людини, що, у свою чергу, потребує змінити підходи до промислових технологій [1]. Проблема кібер-фізичних систем (КФС) з точки зору безперервного генерування великих обсягів даних, який вимагає обробки і візуалізації, що дає можливість підвищити масштабованість, безпеку і ефективність КФС з метою досягнення повної автономії [1].

В таких умовах між людиною і об’єктом праці поміщаються складні технічні засоби, за допомогою яких вона, виконуючи складні моторні та уявні операції, слідуючи запропонованому алгоритму діяльності, впливає на об’єкт. При цьому технічні засоби, як правило, виконані у вигляді автоматизованих робочих місць і містять пульт керування, засоби вводу/виводу інформації та органи керування, що забезпечується через так званий людино-машинний інтерфейс.

Інтенсивний розвиток даної структури залучає користувача у використання великої кількості різноманітних інформаційних сервісів, що вимагають обов'язкової авторизації і аутентифікації, у зв’язку з розподілом функцій (адміністратор, оператор) та необхідності збереження цілісності та достовірності інформації. У більшості систем для ідентифікації користувача застосовується метод встановлення відповідності між логічним ім'ям і введеним паролем.

На сьогоднішній день використання паролів є одним з найпопулярніших способів аутентифікації користувачів в інтернеті. Через способів зберігання паролів, розробники змушені накладати обмеження на те, які паролі безпечніше використовувати. Так, наприклад, найчастіше пароль повинен містити не менше 8 символів, мати літери різних регістрів, містити спеціальні символи і т. д. Можна констатувати, що з часом, ці

обмеження тільки посилюються, а це в свою чергу ускладнює вибір безпечного і одночасно легко запам'ятовується пароля. Так, наприклад, найбільш безпечний пароль буде містити 128 символів з максимальною ентропією. Кількість такої інформації, необхідної для запам'ятовування користувачем, велике, тим більше, що для кожного ідентифікаційного запису рекомендують використовувати унікальний пароль.

Це спричиняє необхідність створення умов безпечного зберігання персональних ідентифікаційних даних [1]. Символьні паролі є широко поширеним методом аутентифікації користувачів. Є два основних правила безпечного використання символьних паролів: використовувати тільки паролі, які важко підібрати по словнику і не використовувати однакові або схожі паролі в різних сервісах.

Але при поточній кількість використовуваних користувачами сервісів ці правила практично неможливо виконати без використання додаткових засобів, таких як менеджери паролів.

Однак безліч досліджень показують, що користувачі часто вибирають прості для вгадування паролі або однакові паролі для кількох акаунтів/сервісів.

Сучасні менеджери паролів, в основному, вирішують лише завдання зберігання паролів, але не введення. Однак, відсутність можливості автоматизовано ввести пароль може привести користувача до вибору найменш складного для введення пароля, що зменшить стійкість пароля.

З метою вирішення цієї проблеми розроблена система для безпечного зберігання та автоматизованого введення символьних паролів, що складається з комплексу програм, протоколів і пристроїв. Система являє собою два пристрої, що обмінюються даними через Bluetooth. Один з пристроїв емулює клавіатуру і приєднується через USB до комп'ютера, на який треба ввести пароль. Інший пристрій служить для вибору пароля, який потрібно ввести.

Висновки: Для розробки власного зручного менеджера паролів, розрахованого на зберігання великої кількості облікових даних і одночасну роботу великої кількості користувачів, необхідно проаналізувати програмні системи зберігання паролів, які можуть не підходити для використання в організаціях середнього або більшого розмірів, так як мають істотні недоліки, проаналізувати їх функціонал, виявити найбільш важливі критерії.

Література: 1. Nevliudov, I., Yevsieiev, V., Demska, N., Novoselov, S. (2020). Development of a software module for operational dispatch control of production based on cyber-physical control systems. *Innovative technologies and scientific solutions for industries*, (4 (14), 155-168; 2. Шологон Ю. З. (2015) Проблеми апаратного захисту у кіберфізичних системах. *Lviv Polytechnic National University Institutional Repository* http://ena.lp.edu.ua. С. 138-143