ПІДВИЩЕННЯ НАДІЙНОСТІ БІОМЕТРИЧНИХ СИСТЕМ АВТЕНТИФІКАЦІЇ ШЛЯХОМ ЗАХИСТУ БАЗ ДАНИХ ВІД СУЧАСНИХ КІБЕРЗАГРОЗ

Лавренчук А.А., Пастушенко М.С., Файзулаєв Т.А.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна

E-mail: andrii.lavrenchuk@nure.ua
mykola.pastushenko@nure.ua
Timfai87@gmail.com

Abstract

The study has developed and justified a set of measures aimed at enhancing the security and reliability of biometric authentication systems. The proposed solutions include the use of both symmetric encryption and asymmetric encryption of biometric templates in order to ensure their confidentiality even in the event of a database compromise. Additionally, hashing with the use of salt values and Secure Hash Algorithm 3 (SHA-3) family algorithms is recommended to make it impossible to reconstruct the original biometric data even if the hash values are obtained by an attacker. Multi-level access control, implemented through the Role-Based Access Control (RBAC) model and the Attribute-Based Access Control (ABAC) model, ensures clear regulation of user privileges and administrator privileges. The introduction of auditing mechanisms and access logging systems makes it possible to detect unauthorized activities and to carry out a thorough investigation of security incidents. To reduce the risk of attack propagation within the information system, measures of network segmentation and network isolation are proposed, along with protection mechanisms against

Вступ

З розвитком цифрових технологій біометричні системи автентифікації стали одним із ключових інструментів забезпечення інформаційної безпеки в банківській, урядовій, військовій, освітній та інших сферах. Їх основна перевага полягає в унікальності біометричних характеристик користувача — відбитків пальців, райдужної оболонки ока, геометрії обличчя, голосу та інших параметрів. Водночас, із зростанням масштабів впровадження таких систем пропорційна збільшується кількість кіберзагроз, зокрема тих, що спрямовані на компрометацію баз даних біометричних шаблонів.

Сучасні загрози для біометричних систем автентифікації

На відміну від паролів чи апаратних токенів, біометричні дані неможливо змінити у випадку їх витоку. Це означає, що компрометація навіть однієї бази даних може мати незворотні наслідки для користувача. Сучасні атаки на біометричні системи автентифікації переважно зосереджуються на вразливостях баз даних – атаках типу «ін’єкція структурованої мови запитів» (Structured Query Language Injection, SQL Injection), атаках типу «людина посередині» (Man-in-the-Middle), експлуатації ненадійних прикладних програмних інтерфейсів (Application Programming Interface, API), а також отриманні доступу до нешифрованих біометричних шаблонів [1].

Метою даного дослідження є підвищення надійності біометричних систем автентифікації шляхом виявлення вразливостей у базах даних та впровадження комплексу багаторівневих засобів захисту. У ході роботи було здійснено аналіз архітектур біометричних систем автентифікації, зокрема моделей із централізованим та розподіленим зберіганням шаблонів, а також досліджено процеси зберігання, обробки та передачі біометричних даних [2].

Моделювання векторів атак

Було змодельована типові вектори атак, включаючи ін'єкції структурованої мови запитів (SQL Injection), несанкціонований доступ, внутрішні витоки, міжмережеві атаки та перехоплення даних на етапі їх передачі. Для нейтралізації цих загроз запропоновано такі заходи.

1) Використання симетричного шифрування та асиметричного шифрування біометричних шаблонів, що гарантує їхню конфіденційність навіть у разі компрометації сховища [3].

2) Хешування з використанням сольових значень та алгоритмів родини Secure Hash Algorithm 3 (SHA-3), яке унеможливлює відновлення оригінальних даних зі збережених хешів.

3) Багаторівневий контроль доступу, реалізований через модель контролю доступу на основі ролей (Role-Based Access Control, RBAC) та модель контролю доступу на основі атрибутів (Attribute-Based Access Control, ABAC), що забезпечує чітке розмежування прав користувачів і адміністраторів.

4) Аудит та журналювання доступу з автоматизованим аналізом аномальної активності.

5) Сегментація мережі та ізоляція мережевих зон для запобігання горизонтальному переміщенню зловмисника у внутрішньому середовищі інформаційної системи.

6) Захист від ін'єкцій структурованої мови запитів (SQL Injection) та інших ін'єкційних атак як на рівні програмного забезпечення, так і на рівні системи управління базами даних (СУБД).

7) Регулярне резервне копіювання та розробка процедур відновлення даних, що забезпечує стійкість до технічних збоїв та атак типу «вимагач» (Ransomware).

8) Використання протоколів безпечної передачі Transport Layer Security версії 1.3 (TLS 1.3) для збереження цілісності та конфіденційності даних під час їх обміну між компонентами системи [4].

Висновки

Отримані результати показали, що використання комплексного підходу, який поєднує криптографічні методи, організаційні методи та мережеві методи захисту, суттєво знижує ймовірність успішної компрометації критично важливих даних.

На основі проведених досліджень сформовано рекомендації щодо архітектури безпечних біометричних систем автентифікації з урахуванням принципів моделі «нульової довіри» (Zero Trust), поділу повноважень адміністратора бази даних і системного адміністратора, а також відповідності міжнародним стандартам інформаційної безпеки — ISO/IEC 27001 «Системи управління інформаційною безпекою» та ISO/IEC 24745 «Біометрія. Захист біометричної інформації».

Перспективними напрямами подальшої роботи є впровадження гомоморфного шифрування, яке дає змогу здійснювати обробку біометричних шаблонів без необхідності їх розшифрування, а також інтеграція з рішеннями класу систем управління інформаційною безпекою та подіями (Security Information and Event Management, SIEM) для автоматизованого моніторингу та виявлення інцидентів безпеки в реальному часі.

Література

1. Бондаренко, М. В. Інформаційна безпека держави / М. В. Бондаренко. – Київ : Нац. ун-т охорони здоров'я України імені П. Л. Шупика, 2022.

2. Петров, І. О. Криптографічні технології в системах автентифікації / І. О. Петров, Л. М. Коваленко. – Харків : ХНУРЕ, 2020.

3. Гаврилюк, В. С. Методи захисту біометричних даних у сучасних інформаційних системах / В. С. Гаврилюк, О. В. Сахно. – Київ : НАУ, 2021.

4. Безуглий, М. П. Захист баз даних від сучасних кіберзагроз / М. П. Безуглий, С. І. Тарасенко. – Одеса : ОНПУ, 2023.