УДК 004.56.5(043.2)

А. В. Вовковинська
І.С. Колесник

Порівняння аутентифікації та авторизації у сучасних системах захисту інформації.

Вінницький національний технічний університет

Анотація

Зв'язок між аутентифікацією та авторизацією в сучасних системах захисту інформації - це важливий аспект забезпечення безпеки даних. Аутентифікація встановлює особистість користувача, використовуючи різноманітні методи, тоді як авторизація надає контроль над рівнем доступу після успішної перевірки. Ці дві складові є ключовими для захисту конфіденційності та цілісності інформації у сучасних інформаційних системах Дослідження цих аспектів дозволить докладно проаналізувати та порівняти аутентифікацію та авторизацію у системах захисту інформації, їх переваги та обмеження в сучасному світі технологій.

Ключові слова: аутентифікація, авторизація, системи захисту інформації.

Abstract

The connection between authentication and authorization in modern information security systems is an important aspect of data security. Authentication establishes the identity of the user using a variety of methods, while authorization provides control over the level of access after successful verification. These two components are key to protecting the confidentiality and integrity of information in modern information systems. The study of these aspects will allow to analyze in detail and compare authentication and authorization in information protection systems, their advantages and limitations in the modern world of technology.

Keywords: authentication, authorization, information security systems.

Вступ

Технології аутентифікації та авторизації в сучасних системах захисту інформації виявляються ключовими складовими для забезпечення безпеки даних. Однак, із зростанням кількості методів аутентифікації з'являються нові виклики, такі як вразливості та витоки даних. Тому актуальним стає пошук оптимальних методів, які забезпечують високий рівень захисту та забезпечують зручність для користувачів.

У сучасному цифровому світі, де обмін інформацією відіграє ключову роль у всіх сферах діяльності, забезпечення безпеки даних стає невід'ємною складовою. Одним із фундаментальних аспектів забезпечення цілісності, конфіденційності та доступності інформації є правильна і ефективна реалізація процесів аутентифікації та авторизації.

Аутентифікація визначає, хто саме має доступ до системи чи інформації, перевіряючи ідентичність користувача через різноманітні методи, включаючи паролі, біометрію та інші механізми. Спрощено кажучи, це процес перевірки "хто я є".

З іншого боку, авторизація визначає, що саме ця ідентифікована особа чи сутність може робити з отриманими дозволами в системі після успішної аутентифікації. Це вже встановлює рівень доступу та повноважень користувача.

Розуміння та вдала імплементація цих процесів в сучасних системах захисту інформації відіграють критичну роль у запобіганні несанкціонованому доступу, зловживанню правами та збереженні конфіденційності даних. В контексті швидкозмінюваної технологічної парадигми, дослідження та вдосконалення цих аспектів є ключовим завданням для забезпечення надійного захисту інформації у сучасному цифровому світі.

Результати досліджень

Авторизація є функцією визначення прав доступу до ресурсів і управління цим доступом. Важливо зазначити, що це не те ж саме що ідентифікація та аутентифікація: ідентифікація - це називання особою

себе системі; аутентифікація - це встановлення відповідності особи, призначеному ним самим ідентифікатором; а авторизація - надання цій особі можливостей у відповідність до покладених йому правами або перевірка наявності прав при спробі виконати будь-яку дію. Наприклад, авторизацією є ліцензії на здійснення певної діяльності.

Авторизація включає в себе такі аспекти:

1. Рівні доступу: різні користувачі можуть мати різні рівні доступу в системі. Наприклад, у системі управління проектами звичайні користувачі можуть мати доступ лише до читання даних, тоді як адміністратори мають повний доступ до редагування та видалення інформації. Або, скажімо, у системі електронної медичної документації, лікарі можуть мати вищий рівень доступу, ніж медичні сестри чи адміністративний персонал.
2. Дозволи на доступ: перевірка також визначає конкретні дії, які користувач може здійснювати. Це можуть бути дозволи на читання, запис, зміну або видалення певних даних. Наприклад, в онлайн-магазинах, адміністратори мають дозвіл на управління асортиментом товарів, тоді як звичайні користувачі можуть лише переглядати товари та робити замовлення.
3. Часові обмеження: це про тимчасові рамки доступу. Наприклад, деякі користувачі можуть мати доступ тільки в певний час доби або в певні дні тижня.

Цей процес перевірки не тільки забезпечує безпеку даних, а й допомагає ефективно використовувати ресурси, надаючи користувачам тільки ті можливості, які необхідні для їхньої роботи, і встановлюючи необхідні обмеження для підтримки безпеки системи.

Аутентифікація - підтвердження достовірності чого-небудь або кого небудь. Наприклад, пред'явлення паспорта - це підтвердження автентичності заявленого імені по батькові.

Існує кілька методів такої перевірки, призначених для підвищення безпеки:

1. Введення логіна і пароля: від користувача вимагається ввести унікальний логін і пароль, які пов’язані з його акаунтом. Це один із найпоширеніших способів аутентифікації.
2. Багатораторна автентифікація (MFA): користувач повинен надати кілька форм підтвердження своєї особи. Наприклад, після введення логіна і пароля, він може отримати одноразовий код на свій телефон або електронну пошту, який також необхідний для входу.
3. Біометричні дані: цей метод уже використовує унікальні фізіологічні або поведінкові характеристики користувача, такі як відбитки пальців, розпізнавання обличчя або голосу. Має високий рівень безпеки, оскільки біометричні дані складно підробити або вкрасти.
4. Перевірка через соціальні мережі: дає змогу користувачам увійти на сайт або в застосунок, використовуючи свої облікові дані із соціальних мереж, як-от Facebook або Google.

Основна різниця між цими двома процесами полягає в тому, що перший підтверджує особу користувача, тоді як другий визначає, що цей користувач може робити після підтвердження його особистості. Розуміння цієї відмінності є ключовим, оскільки без належної автентифікації авторизація стає невиправданою – система не може переконатися, що користувач з правильними дозволами справді є тим, за кого себе видає.

Нижче наведено таблицю, в якій детально висвітлені головні відмінності та схожості між автентифікацією та авторизацією:

Таблиця 1 – Таблиця відмінносейі та схожостей між автентифікацією та авторизацією

Аспект	Автентифікація	Авторизація
Визначення	Перевірка особистості користувача.	Керування доступом користувача до ресурсів після перевірки.
Ціль	Посвідчення, що користувач є тим, за кого він себе видає.	Керування діями та доступом користувача в системі.
Процес	Підтвердження особи через введення даних (логіна, пароля), біометричні дані тощо.	Визначення дозволів і рівня доступу користувача до ресурсів.
Фокус	Посвідчення особи користувача.	Визначення прав доступу та контроль над функціональністю.
Ключові моменти	Логін, пароль, біометричні дані, одноразові коди тощо.	Рівні доступу, дозволи на дії, тимчасові обмеження тощо.
Припускає	Попередню аутентифікацію для визначення особи.	Успішну аутентифікацію для встановлення доступу до ресурсів.
Чому важливо	Запобігає несанкціонованому доступу до системи та даних.	Контролює, що користувач може робити в системі після аутентифікації.
Приклад у житті	Введення пароля під час входу в акаунт, використання відбитків пальців або розпізнавання обличчя.	Після входу в пошту, визначення, чи може користувач писати, читати, видаляти листи.
Схожості	Обидва процеси пов’язані з безпекою даних і контролем доступу.	Обидва процеси працюють у парі, визначаючи, хто має доступ до чого.

Враховуючи різні необхідні аспекти при використанні автентифікації та авторизації варто розглянути конкретні приклади, де використовується той чи інший метод.

1. Банківські системи: доступ до онлайн-банкінгу або мобільних додатків банків, користувачі перш за все автентифікують свою особу, вводячи логін та пароль. Після успішної перевірки система визначає, які операції (авторизації) може виконувати користувач, такі як переказ коштів, оплата рахунків чи перегляд балансу.
2. Соціальні мережі: вхід в особистий акаунт в соціальній мережі, ви підтверджуєте свою особу (аутентифікація), зазвичай, вводячи логін та пароль. Після цього система визначає, які профілі та повідомлення ви можете переглядати чи редагувати, а також яку інформацію ви можете публікувати.
3. Електронна пошта: вхід в поштову скриньку ви підтверджуєте свою особу (аутентифікація). Надалі, на основі авторизації, система надає вам можливість читати, писати, видаляти та надсилати повідомлення.
4. Онлайн-магазини: оформлення замовлення в інтернет-магазині, система аутентифікує вас і потім авторизує певні дії, такі як додавання товарів у кошик, оплата та управління замовленнями.
5. Медичні інформаційні системи: лікарі можуть автентифікувати себе, щоб отримати доступ до медичної історії пацієнтів, при цьому авторизація визначає, які дані вони можуть бачити та змінювати.

Зважаючи на важливість безпечної роботи з інформацією, аутентифікація та авторизація є вирішальними елементами в сучасних системах захисту інформації. Аутентифікація підтверджує особисту ідентичність користувача, тоді як авторизація визначає права доступу після підтвердження особистості. Ці процеси використовуються у банківському секторі, соціальних мережах, електронній пошті та багатьох інших сферах для забезпечення конфіденційності та безпеки інформації. Усвідомлення різниці між цими процесами є ключовим для забезпечення безпеки даних та правильного управління доступом до ресурсів.

Висновок

Аутентифікація та авторизація є ключовими елементами безпеки даних у сучасних системах. Аутентифікація підтверджує особу користувача, а авторизація визначає права доступу після підтвердження особистості. Ці процеси взаємопов'язані та працюють разом для забезпечення безпеки даних.

Для підвищення рівня безпеки даних необхідно використовувати надійні методи аутентифікації, регулярно змінювати паролі та інші облікові дані, уважно ставитися до підозрілих електронних листів та посилань, встановлювати актуальні антивірусні програми та брандмауери, а також регулярно проводити аудит систем безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ / REFERENCES

1. Ідентифікація та аутентифікація користувачів. Розмежування доступу зареєстрованих користувачів до ресурсів автоматизованих систем. [Електронний ресурс] – Режим доступу до ресурсу: https://classmill.com/659/112/m/2YRmy.
2. У чому різниця між процесами аутентифікації та авторизації. [Електронний ресурс] – Режим доступу до ресурсу: https://foxminded.ua/riznytsia-mizh-avtentyfikatsiieiu-ta-avtoryzatsiieiu/.
3. Технології захисту інформації: навчальний посібник [Ю. А. Тарнавський] – Вінниця: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
4. Комплексні системи захисту інформації : навчальний посібник / К63 [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2018. – 118 с.
5. Технології захисту інформації: навчальний посібник [С. Е. Остапов, С. П. Євсеєв, О. Г. Король.] – Харків: Вид. ХНЕУ, 2013. – 476 с.

Вововковинська Аліна Вадимівна – студентка групи 2КІ-21б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: alinvovkov@gmail.com

Колесник Ірина Сергіївна – к.т.н., доцент кафедри обчислювальної техніки, Вінницький національний технічний університет, Вінниця, e-mail: kolesnyk.iryna@vntu.edu.ua.

Vovokovynska Alina - student of the 2CE-21b group, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: alinvovkov@gmail.com.

Kolesnyk Iryna - PhD., Associate Professor of Computer Engineering, Vinnitsa National Technical University, Vinnitsa, e-mail: kolesnyk.iryna@vntu.edu.ua.