УДК 004.056

В. М. Зінченко
І. В. Богач

АНАЛІЗ СУЧАСНИХ МЕТОДІВ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

Вінницький національний технічний університет

Анотація

У роботі було розглянуто проблему аутентифікації користувачів у сучасних інформаційних системах. Було описано різні методи аутентифікації, їхні переваги та недоліки, а також проаналізовано актуальні проблеми безпеки в цій сфері.

Ключові слова: автентифікація користувачів, методи автентифікації, безпека інформаційних систем, захист даних.

Abstract

This paper considers the problem of user authentication in modern information systems. Different methods of authentication, their advantages and disadvantages were described, and current security issues in this area were analyzed.

Keywords: user authentication, authentication methods, information systems security, data protection.

Вступ

У сучасну епоху, де інформація стає все більш цінною, а її зберігання та обробка дедалі більше відбуваються в електронному вигляді, питання безпеки та захисту даних набувають першочергової ваги. Аутентифікація користувачів, яка слугує для ідентифікації та авторизації користувачів для доступу до систем та ресурсів, є одним з ключових елементів забезпечення загальної безпеки. Програмні сервіси аутентифікації відіграють важливу роль у цьому процесі, пропонуючи надійні та зручні механізми для верифікації особистості користувачів.

Результати дослідження

Автентифікація користувачів - це метод, який запобігає доступу неавторизованих користувачів до конфіденційної інформації. Наприклад, користувач А має доступ лише до необхідної інформації і не може бачити конфіденційну інформацію користувача Б.

Кіберзлочинці можуть отримати доступ до системи і викрасти інформацію, якщо автентифікація користувача не захищена. Витоки даних, з якими зіткнулися такі компанії, як Adobe, Equifax та Yahoo, є прикладами того, що відбувається, коли організації не можуть захистити автентифікацію користувачів.

Хакери отримали доступ до облікових записів користувачів Yahoo, щоб викрасти контакти, календарі та приватні електронні листи в період з 2012 по 2016 рік. Витік даних Equifax у 2017 році призвів до витоку даних кредитних карток понад 147 мільйонів споживачів. Без безпечного процесу автентифікації будь-яка організація може опинитися в зоні ризику.

Автентифікація - це термін, який позначає процес доведення того, що певний факт або документ є справжнім. У комп'ютерних науках цей термін зазвичай асоціюється з підтвердженням особи користувача. Зазвичай користувач підтверджує свою особу, надаючи свої облікові дані, тобто узгоджену інформацію, якою обмінюються користувач і система.

Кіберзлочинці постійно вдосконалюють свої атаки. Як наслідок, команди безпеки стикаються з безліччю проблем, пов'язаних з автентифікацією. Саме тому компанії починають впроваджувати більш складні стратегії реагування на інциденти, включаючи автентифікацію як частину цього процесу. У наведеному нижче списку розглядаються деякі поширені методи автентифікації, що використовуються для захисту сучасних систем.

1. Автентифікація на основі пароля.

Паролі - найпоширеніший метод автентифікації. Паролі можуть бути у вигляді рядка букв, цифр або спеціальних символів. Щоб захистити себе, потрібно створювати надійні паролі, які включають комбінацію всіх можливих варіантів.

Однак паролі схильні до фішингових атак і поганої гігієни, що послаблює їх ефективність. Середньостатистична людина має близько 25 різних облікових записів в Інтернеті, але лише 54% користувачів використовують різні паролі для своїх акаунтів.

Справа в тому, що потрібно пам'ятати дуже багато паролів. Як наслідок, багато людей обирають зручність, а не безпеку. Більшість людей використовують прості паролі замість того, щоб створювати надійні паролі, тому що їх легше запам'ятати.

Суть в тому, що паролі мають багато слабких місць і не є достатніми для захисту інформації в Інтернеті. Хакери можуть легко вгадати облікові дані користувача, перебираючи всі можливі комбінації, поки не знайдуть збіг.

2. Багатофакторна автентифікація

Багатофакторна автентифікація (БФА) - це метод автентифікації, який вимагає двох або більше незалежних способів ідентифікації користувача. Приклади включають коди, згенеровані на смартфоні користувача, тести Captcha, відбитки пальців, голосову біометрію або розпізнавання обличчя.

Методи та технології автентифікації MFA підвищують довіру користувачів, додаючи кілька рівнів безпеки. MFA може бути хорошим захистом від більшості зломів акаунтів, але має свої підводні камені. Люди можуть втратити свої телефони або SIM-карти і не мати можливості згенерувати код автентифікації.

3. Автентифікація на основі сертифікатів

Технології автентифікації на основі сертифікатів ідентифікують користувачів, машини або пристрої за допомогою цифрових сертифікатів. Цифровий сертифікат - це електронний документ, подібний до водійського посвідчення або паспорта.

Сертифікат містить цифрову ідентифікацію користувача, включаючи відкритий ключ, і цифровий підпис центру сертифікації. Цифрові сертифікати підтверджують право власності на відкритий ключ і видаються лише центром сертифікації.

Користувачі надають свої цифрові сертифікати під час входу на сервер. Сервер перевіряє достовірність цифрового підпису та центру сертифікації. Потім сервер використовує криптографію, щоб підтвердити, що користувач має правильний приватний ключ, пов'язаний з сертифікатом.

4. Біометрична автентифікація

Біометрична автентифікація - це процес забезпечення безпеки, який спирається на унікальні біологічні характеристики людини.

Ось ключові переваги використання технологій біометричної автентифікації:

- Біологічні характеристики можна легко порівняти з авторизованими характеристиками, збереженими в базі даних.
- Біометрична автентифікація може контролювати фізичний доступ при встановленні на воротах і дверях.
- Ви можете додати біометричні дані до процесу багатофакторної автентифікації.

Технології біометричної автентифікації використовуються споживачами, урядами та приватними корпораціями, включаючи аеропорти, військові бази та національні кордони.

Ця технологія набуває все більшого поширення завдяки можливості досягти високого рівня безпеки, не створюючи при цьому перешкод для користувача. До поширених методів біометричної автентифікації належать:

- Розпізнавання обличь - зіставлення різних характеристик обличчя людини, яка намагається отримати доступ до затвердженого обличчя, що зберігається в базі даних. Розпізнавання обличчя може бути непослідовним, якщо порівнювати обличчя під різними кутами або порівнювати людей, які виглядають схоже, наприклад, близьких родичів. Живість обличчя, як і пасивна живість обличчя ID R&D, запобігає підробці.

- Сканери відбитків пальців - зіставляють унікальні візерунки на відбитках пальців людини. Деякі нові версії сканерів відбитків пальців можуть навіть оцінювати судинні візерунки на пальцях людини. Наразі сканери відбитків пальців є найпопулярнішою біометричною технологією для пересічних споживачів, незважаючи на їхні часті неточності. Таку популярність можна пояснити появою iPhone.

- Розпізнавання голосу - також відоме як голосова біометрія, досліджує мовленнєві патерни мовця для формування специфічних форм і якостей звуку. Пристрій із голосовим захистом зазвичай покладається на стандартизовані слова для ідентифікації користувачів, як і пароль.

- Сканери очей - включають такі технології, як розпізнавання райдужної оболонки ока та сітківки. Сканери райдужної оболонки направляють яскраве світло в око і шукають унікальні візерунки в кольоровому кільці навколо зіниці ока. Потім вони порівнюються із затвердженою інформацією, що зберігається в базі даних. Автентифікація за допомогою очей може мати неточності, якщо людина носить окуляри або контактні лінзи.

5. Автентифікація на основі токенів

Технології автентифікації на основі токенів дозволяють користувачам вводити свої облікові дані один раз і отримувати натомість унікальний зашифрований рядок випадкових символів. Ви можете використовувати токен для доступу до захищених систем замість того, щоб вводити свої облікові дані знову і знову. Цифровий токен підтверджує, що у вас вже є дозвіл на доступ. Варіанти використання автентифікації на основі токенів включають RESTful API, які використовуються багатьма фреймворками та клієнтами.

Висновки

Технології автентифікації постійно змінюються. Компанії повинні вийти за рамки паролів і розглядати автентифікацію як засіб покращення користувацького досвіду. Такі методи автентифікації, як біометрія, усувають необхідність запам'ятовувати довгі та складні паролі. Завдяки вдосконаленим методам і технологіям автентифікації зловмисники не зможуть використовувати паролі, а витік даних буде попереджено.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Як захистити свій сайт від злому. Топ-10 розповсюджених варіантів злому. [Електронний ресурс]. – Режим доступу: https://fondy.ua/uk/blog/how-toprotect-website/
2. Загрози при роботі в Інтернеті і їх уникнення. [Електронний ресурс] – Режим доступу: https://naurok.com.ua/zagrozi-pri-roboti-v-interneti-i-huniknennya-257244.html
3. Двофакторна аутентифікація користувача – як це працює. [Електронний ресурс]. – Режим доступу: https://hosting.in.ua/ua/articles/bezopasnost/dvukhfaktornaya-autentifikatsiya-polzovatelya-kak-eto-rabotaet/
4. Автентифікація користувачів [Електронний ресурс] – Режим доступу: https://strojsoc.ptu.org.ua/wp-content/uploads/2020/04/%D0%90%D1%81-93_2_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0.pdf

Зінченко Вероніка Максимівна — студентка групи 1ІСТ-20б, кафедра автоматизації та інтелектуальних інформаційних технологій, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, м.Вінниця, e-mail: zinchenkoveronicamaksimivna@gmail.com.

Богач Ілона Віталіївна **–** к.т.н., доцент кафедри автоматизації та інтелектуальних інформаційних технологій, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, м.Вінниця, e-mail: ilona.bogach@gmail.com

Zinchenko Veronika Maksimivna — student of 1IST-20b group, Department of Automation and Intelligent Information Technologies, Faculty of Intelligent Information Technology and Automation, Vinnytsia National Technical University, Vinnytsia, e-mail: zinchenkoveronicamaksimivna@gmail.com.

Bogach Ilona Vitaliivna – Associate Professor of Automation and Intelligent Information Technologies Department, Faculty of Intelligent Information Technology and Automation, Vinnytsia National Technical University, Vinnytsia, e-mail: ilona.bogach@gmail.com