Міністерство освіти і науки України
Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Національний університет «Львівська політехніка»

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
IV Всеукраїнської науково-практичної конференції
молодих учених, студентів і курсантів

27 листопада 2020 року

Львів – 2020

ББК 32.81+78.362

*Інформаційна безпека та Інформаційні технології: з*бірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 27 листопада 2020 року. Львів, ЛДУ БЖД, 2020, 249 с.

За точність наведених фактів, самостійність наукового аналізу та нормативність стилістики викладу, а також за використання відомостей, що не рекомендовані до відкритої публікації відповідальність несуть автори опублікованих матеріалів.

Секція 1
КІБЕРБЕЗПЕКА

УДК 004.056.53

АНАЛІЗ ПРИНЦИПІВ РЕАЛІЗАЦІЇ МЕТОДІВ ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ В СУЧАСНИХ ПРОГРАМНИХ ДОДАТКАХ

Самара Н. М., Бурак Н. Є.
Львівський державний університет безпеки життєдіяльності, Львів

У роботі здійснено огляд сучасних методів автентифікації та проведено аналіз принципів реалізації методів двофакторної автентифікації в сучасних програмних додатках

Ключові слова: *автентифікація, захист, програмні модулі, інформація.*

The paper reviews modern methods of authentication and analyzes the principles of two-factor authentication methods implementation into modern software applications

Keywords: *authentication, protection, software modules, information.*

Інтернет є невід'ємною частиною життя сучасної людини. Безперервний стрімкий розвиток даної мережі призводить до збільшення кількості різноманітних веб-застосунків, що використовуються для будь-яких сфер діяльності. Керований доступ до наданих сервісів та персоналізація контенту – в цьому полягає сучасна тенденція створення веб-застосунків.

Поруч з великою кількістю переваг їх застосування, існує і велика кількість недоліків. Вразливості веб-застосунків є одним з найбільш поширених шляхів проникнення в інформаційні системи та витоку особистої інформації користувачів. У зв'язку з цим підвищуються вимоги до методів автентифікації та авторизації клієнтів.

Оскільки, кількість веб-застосунків зростає з кожним днем, і мати окремий логін та пароль для кожного сайту дуже важко для запам'ятовування. Це може призвести або до небезпечного зберігання такої «бази» на персональному комп'ютері користувача, або до використання для всіх сайтів однієї і тієї ж пари (логін, пароль). Існує багато методів підвищення безпеки автентифікації в наш час. Одним з найнадійніших є використання сервісів автентифікації, що розроблені згідно світових стандартів автентифікації.

Незважаючи на простоту у використанні, застосування цих додатків значно сприяє унеможливленню несанкціонованого входу до інформаційної системи.

Загалом, методи автентифікації діляться на три категорії: слабка (однофакторна), сильна (багатофакторна) та строга автентифікацію.

Слабкою називають однофакторну автентифікацію за допомогою пароля. На стійкість даного методу автентифікації значною мірою впливає людський чинник.

Сильною або багатофакторною називають автентифікацію, що використовує декілька факторів автентифікації.

Існує всього три типи факторів:

– фактор знання;

– фактор володіння;

– фактор властивості.

Строга автентифікація є різновидом багатофакторної автентифікації. Ідея строгої автентифікації, що реалізується в криптографічних протоколах, полягає в наступному. Користувач доводить свою автентичність інформаційній системі демонструючи знання будь-якого секрету, який, наприклад, може бути попередньо розподілений безпечним способом між сторонами автентифікаційного обміну. На даний момент строга автентифікація є найбільш стійкою, однак, незважаючи на це, вона не є стійкою до атак, які направлені на мережу чи власне апаратне забезпечення.

Для впровадження строгої автентифікації використовують сервіси автентифікації. Реалізації представлені компаніями-гігантами, наприклад, як Google та Microsoft надають впевненість в їх коректності та стійкості обраних ними факторів автентифікації. Далі розглянемо дані сервіси автентифікації.

Google Authenticator – мобільний застосунок, що використовується для виконання двофакторної автентифікації, в облікових записах Google та сторонніх сервісах. Реалізований для декількох мобільних платформ, не має можливості ініціалізації на декількох пристроях. Секретний ключ можна інтегрувати в застосунок як QR-код, або ввести вручну. Налаштування в застосунку представлені лише засобами синхронізації часу з серверами Google. Автентифікатор генерує 6-ти або 8-мизначний одноразовий пароль, з використанням відкритих стандартів алгоритмів HOTP та TOTP. Дані паролі використовуються в якості другого фактору автентифікації і вводяться після коректного введення логіну та паролю. Пароль дійсний протягом 30 секунд, що запобігає використанню його кілька разів.

Microsoft Authenticator – мобільний застосунок, який допомагає входити в облікові записи, виконуючи двофакторну автентифікацію. Працює з будь-яким обліковим записом, який використовує двофакторну автентифікацію та підтримує одноразові паролі (TOTP).

Даний додаток можна використовувати кількома способами, включаючи:

1. Після входу з іменем користувача та паролем в застосунок надходить запит на автентифікацію.

2. Вхід без введення пароля, використовуючи ім'я користувача, застосунок автентифікації та мобільний пристрій, використовуючи відбиток пальця, обличчя або PIN-код.

3. Як генератор коду для будь-яких облікових записів, які підтримують програми автентифікації.

В якості генератора кодів Microsoft Authenticator генерує шестизначний пароль, який відображається під кожним доданим обліковим записом. Пароль дійсний протягом 30 секунд, що запобігає використанню коду кілька разів. Ініціалізація облікового запису проходить шляхом сканування QR-коду, або введення коду вручну. Не має можливості ініціалізувати один обліковий запис в декількох застосунках на різних пристроях одночасно.

Отже, у загальних принципах, Google Authenticator і Microsoft Authenticator виконують однакову роботу і працюють подібними способами. Однак необхідно відзначити, що Microsoft пропонує більш комплексний продукт. Це не тільки можливість синхронізації декількох пристроїв, але і можливість створення резервної копії, яка буде важливою, якщо користувачеві коли-небудь потрібно буде отримати новий телефон. Крім того, якщо користувач щодня користується продуктами Microsoft, використання автентифікатора від того самого розробника полегшує підключення до відповідних облікових записів - користувачам просто потрібно натиснути сповіщення.

Інформаційні джерела

1. Чунарьова А. В. Аналіз існуючих шаблонів систем автентифікації в інформаційно-комунікаційних системах та мережах / А. В. Чунарьова, А. В. Чунарьов // Безпека інформації: наук.-практ. журнал. – 2012. – № 2 (18). – С. 65–70.

2. Ляшенко, Г.Є & Астраханцев, А.А. (2017). Дослідження ефективності методів біометричної автентифікації. Системи обробки інформації. 2(148). 111-114. https://doi.org/10.30748/soi.2017.148.20

3. Иванов Вадим Вадимович, Лубова Елена Сергеевна, and Черкасов Денис Юрьевич. "Аутентификация и авторизация" Проблемы современной науки и образования, no. 2 (84), 2017, pp. 31-33.

4. Мушинський А.О. Інформаційна безпека пристроїв IoT // Проблеми та перспективи розвитку системи безпеки життєдіяльності: Зб. наук. праць XV Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів. – Львів: ЛДУ БЖД, 2020. – С. 214-216.

З М І С Т

Секція 1

КІБЕРБЕЗПЕКА

Напрям 1. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Напрям 2. ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Напрям 3. ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Напрям 4. БЕЗПЕКА ІНФОРМАЦІЇ У ХМАРНИХ СХОВИЩАХ

Напрям 5. КРИПТОГРАФІЧНІ ТА СТЕГАНОГРАФІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

Наукове видання

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
IV Всеукраїнської науково-практичної конференції
молодих учених, студентів і курсантів

Відповідальні за випуск **Олександр Придатко**
Ростислав Ткачук

Оригінал-макет **Ростислав Ткачук**

Друк на різографі **Маріанна Климус**

Підписано до друку 12.11.2020 р.
Формат 60×84/16. Гарнітура Times New Roman.
Друк на різографі. Папір офсетний.
Ум. друк. арк. 15,7.

Друк ЛДУ БЖД
79007, Україна, м. Львів, вул. Клепарівська, 35
тел./факс: (032) 233-32-40, 233-24-79.
e- mail: mail@ubgd.lviv.ua, ndr@ ubgd.lviv.ua