УДК 681.12

І. В. Богач[1]
В. С. Збитківський[1]

РОЗРОБКА БАГАТОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧА ВІДЕО СЕРВІСУ

[1] Вінницький національний технічний університет

Анотація

Зроблено огляд способів та інструментів багаторівневого захисту інформації користувача відео сервісу для її безпечної передачі та збереження в базі даних.

Ключові слова: JWT, веб-додатки, Angular, NodeJS, MongoDB, ExpresJS, MFA, програмування веб-додатків.

Abstract

An overview of ways and tools for multi-level protection of user information for its secure transmission and storage in the database.

Keywords: JWT, web-applications, Angular, NodeJS, MongoDB, ExpresJS, MFA, web-applications programming.

Вступ

Захист акаунтів за допомогою одного фактора — складного пароля — близько двох десятків років тому перестав бути надійним. Тому рекомендується використовувати додаткові фактори захисту. Тим більше, що зараз є можливість вибрати оптимальний варіант за запитами, ціною та якістю.

А враховуючи те, що пандемія наклала відбиток на багато сфер соціального життя, у тренді опинилася віддалена робота — раніше улюблений формат IT-компаній, а тепер веб-, маркетингових студій, освітніх ресурсів, call-центрів та інших підприємств, де завдання на 80-90% здійснюються за допомогою комп’ютерів. Однак нюанс у тому, що домашні ПК, на яких найчастіше продовжують віддалено працювати співробітники, потребують такого ж захисту, як і корпоративні пристрої, де може бути встановлене відповідне ПЗ.

Коли ви входите у свої онлайнові облікові записи, ви доводите доказ того, що працюєте саме в службі. Традиційно це зроблено за допомогою імені користувача та пароля. На жаль, це не дуже хороший спосіб зробити це. Імена користувачів часто легко знайти; іноді це лише ваша адреса електронної пошти. Оскільки паролі важко запам'ятати, користувачі, як правило, вибирають прості паролі або використовують однаковий пароль на багатьох різних сайтах.

Результати дослідження

Принцип роботи багатофакторної автентифікації полягає в тому, що при авторизації користувача в операційній системі або в будь-якому обліковому записі, служба запитує підтвердження особи за допомогою додаткових факторів, які має користувач.

Двофакторна автентифікація (ДФА, англ. two-factor authentication, також відома як двоетапна верифікація), є типом багатофакторної аутентифікації. ДФА — представляє собою технологію, що забезпечує ідентифікацію користувачів за допомогою комбінації двох різних компонентів.

Хорошим прикладом двофакторної аутентифікації є авторизація Google і Microsoft. Коли користувач заходить з нового пристрою, крім аутентифікації по імені та паролю, його просять ввести шестизначний (Google) або восьмизначний (Microsoft) код підтвердження. Ви можете отримати його за допомогою SMS, або голосового дзвінка на ваш телефон, він може бути взятий з заздалегідь складеного реєстру разових кодів або ви можете використовувати додаток-аутентифікатор, генеруючий новий одноразовий пароль за короткі проміжки часу. Вибрати один з методів можна в налаштуваннях вашого Google або Microsoft-акаунта.

Багато продуктів з функцією багатофакторної автентифікації вимагають від користувача клієнтське програмне забезпечення, для того, щоб система багатофакторної аутентифікації запрацювала. Деякі розробники створили окремі настановні пакети для входу в мережу, ідентифікаційних даних

веб-доступу VPN-підключення. Щоб використовувати з цими продуктами токен або смарт-карту, потрібно встановити на PC чотири або п'ять пакетів спеціального програмного забезпечення. Це можуть бути пакети, які використовуються для здійснення контролю версії або це можуть бути пакети для перевірки конфліктів з бізнес-додатками. Якщо доступ може бути проведений з використанням веб-сторінок, то тоді можна обійтися без непередбачених витрат. З іншими програмними рішеннями багатофакторної аутентифікації, такими як «віртуальні» токени або деякі апаратні токени, жодне не може бути встановлено безпосередніми користувачами[1].

Багатофакторна аутентифікація не стандартизована. Існують різні форми її реалізації. Отже, проблема полягає в її здатності до взаємодії. Існує багато процесів і аспектів, які необхідно враховувати при виборі, розробці, тестуванні, впровадженні та підтримці цілісної системи управління ідентифікацією безпеки, включаючи всі релевантні механізми аутентифікації і супутніх технологій: це все описав Brent Williams, в контексті «Identity Lifecycle»

Багатофакторна аутентифікація має ряд недоліків, які перешкоджають її поширенню. Зокрема людині, яка не розбирається в цій області, складно стежити за розвитком апаратних токенів або USB-штекерів. Багато користувачів не можуть самостійно встановити сертифіковане програмне забезпечення, так як не володіють відповідними технічними навичками. Загалом, багатофакторні рішення вимагають додаткових витрат на встановлення та оплату експлуатаційних витрат. Багато апаратні комплекси, засновані на токенах, запатентовані, і деякі розробники стягують з користувачів щорічну плату. З точки зору логістики, розмістити апаратні токени важко, так як вони можуть бути пошкоджені або втрачені. Випуск токенів в таких областях, як банки, або інших великих підприємствах повинен бути відрегульований[2]. Крім витрат на установку багатофакторної аутентифікації значну суму також становить оплата технічного обслуговування. В 2008 році великий медіа-ресурс Credit Union Journal провів опитування серед понад 120 кредитних спілок США. Мета опитування — показати вартість технічного обслуговування пов'язану з двофакторної аутентифікацією. У результаті вийшло, що сертифікація програмного забезпечення і доступ до панелі інструментів мають найвищу вартість.

Перевага двофакторної автентифікації через мобільний пристрій: не потрібні додаткові токени, тому що мобільний пристрій завжди під рукою. Код підтвердження постійно змінюється, а це безпечніше, ніж однофакторний логін-пароль[3].

Недоліки двофакторної автентифікації через мобільний пристрій. Мобільний телефон повинен ловити мережу, коли відбувається аутентифікація, інакше повідомлення з паролем просто не дійде. Ви ділитеся з кимось вашим мобільним телефоном, що впливає на ваше особисте життя і може бути в майбутньому на нього буде приходити спам. Текстові повідомлення, які, потрапляючи на ваш мобільний телефон, можуть бути перехоплені. Текстові повідомлення приходять з деякою затримкою, так як деякий час йде на перевірку. Сучасні смартфони використовуються як для одержання пошти, так і для отримання SMS.

Як правило електронна пошта на мобільному телефоні завжди включена. Таким чином, усі акаунти, для яких пошта є ключем, можуть бути зламані (перший фактор). Мобільний пристрій (другий фактор).

Кінцева мета MFA — створити лінію захисту між вашою інформацією і хакерами. Самі сайти, до яких Ви під’єднуєтеся значно ускладнюють доступ стороннім особам. І навіть якщо вони можуть знати ваш пароль, вони не зможуть відтворити другий фактор аутентифікації (ваш відбиток пальця, текстовий код або відповідь на секретне питання)[4].

Висновки

Сьогодні люди очікують, що багатофакторна аутентифікація буде частиною будь-якого налаштування облікового запису. Зараз вона впроваджується як базовий елемент безпеки. MFA забезпечує вищий рівень захисту, ніж просте ім’я користувача та пароль.

Користувачі та клієнти можуть відчувати себе більш цінними компаніями, які використовують MFA. MFA може підключатися за допомогою програмного забезпечення єдиного входу і надавати користувачам простіший та безпечніший процес входу в систему.

Зберігати конфіденційну інформацію в Інтернеті або навіть в хмарі стає все небезпечніше. Зростання кількості випадків використання багатофакторної аутентифікації полегшує життя і компаній, і звичайних людей, а також значно посилює загальний захист від атак.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Angular, AngularIO [Електронний ресурс]. [Веб-сайт].– 2021. – Режим доступу до ресурсу: https://angular.io/docs.
2. NodeJS, Wikipedia [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://uk.wikipedia.org/wiki/Node.js.
3. NgRx, NgRxIO [Електронний ресурс]. [Веб-сайт]. – 2021. – Режим доступу до ресурсу: https://ngrx.io/docs.
4. MFA [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://yubikey.com.ua/shcho-take-bahatofaktorna-avtentyfikatsiia-ta-koly-dotsilno-ii-vykorystovuvaty.

Збитківський Владислав Сергійович *– студент групи 1ПІ-22М, кафедра програмної інженерії, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м.Вінниця, e-mail: vladz15@ukr.net*

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

Zbytkivskyi Vladislav Sergiyvich *– student of 1SE-22m group, Department of Software Engineering, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: vladz15@ukr.net*

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