МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний технологічний університет
Університет Інформатики і прикладних знань, м.Лодзь, Польща
Національний технічний університет України «Київський політехнічний інститут»
Навчально-науковий інститут комп'ютерних систем і технологій «Індустрія 4.0» ім. П.М. Платонова

XXIII Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Матеріали конференції

Одеса

20-21 квітня 2023 р.

Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXIII Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 20-21 квітня 2023 р**.** - Одеса, Видавництво ОНТУ, 2023 р. – 449 с.

Збірник включає матеріали доповідей учасників конференції, які об'єднані за тематичними напрямками конференції.

Збірник буде корисним як для фахівців і працівників фірм, зайнятих в області IT, так і для викладачів, магістрів і студентів вищих навчальних закладів, які навчаються за напрямами і спеціальностями програмного забезпечення, обчислювальної техніки і автоматизованих систем, прикладної математики та обробки інформації, буде корисним професіоналам з комп'ютерного моделювання та розробки комп'ютерних ігор.

Результати досліджень у збірнику представляють собою своєрідний зріз сучасного стану справ в перерахованих галузях знань, який може допомогти як фахівцям, так і студентам університетів скласти загальну картину розвитку інформаційних технологій та пов'язаних з ними питань.

Наукові праці згруповані за напрямками роботи конференції та наведені в алфавітному порядку прізвищ авторів.

Матеріали (тези доповідей) друкуються в авторській редакції. Відповідальність за якість та зміст публікацій несе автор.

Матеріали подано українською та англійською мовами.

Редактор збірника Котлик С.В.

© Одеський національний технологічний університет

налаштовані методи перетворення повідомлень можуть забезпечити надійну передачу даних між пристроями автомобіля, що допомагає уникнути збоїв та помилок у роботі систем.

У той же час, використання нових технологій, таких як Ethernet та розподілені реєстри, може допомогти підвищити продуктивність та гнучкість систем, а також забезпечити кращий захист від загроз безпеки.

Для забезпечення найкращих результатів дослідження методів перетворення повідомлень в автомобільних системах має бути ретельно сплановане та виконане з використанням сучасних технологій та інструментів аналізу даних, таких як DLT-Viewer. Це дозволить оптимізувати продуктивність та безпеку автомобільних систем та зробити автомобілі більш надійними та безпечними для водіїв та пасажирів.

СПИСОК ВИКОРИСТАННОЇ ЛІТЕРАТУРИ

[1]Underwood S. Automated, Connected, and ElectricVehicle Systems: A Textbook: Springer, 2014. 146 p. (дата звернення: 20.03.2023).

[2]Navet N., Automotive Embedded Systems Handbook: Volume 1.: Springer Nature Switzerland AG, 2009. 490 p.

[3]Prytz R., "Machine learning methods for vehicle predictive maintenance using off-board and on-board data ", 2014. 96 p.

УДК 004.056.5

ПРОЦЕС БЕЗПЕЧНОЇ ПЕРЕДАЧІ ІНФОРМАЦІЇ У МОБІЛЬНОМУ ДОДАТКУ “СТУДЕНТ ЧДТУ” З ВИКОРИСТАННЯМ SPRING SECURITY НА ОСНОВІ JWT

КУНИЦЬКА С.Ю. (kunitskaya33@gmail.com)
АРХІПОВ М.О. (m.o.arkhipov.fitis20@chdtu.edu.ua),
ЧОПОВЕНКО В.М. (vasyachopovenko@gmail.com)
Черкаський державний технологічний університет

В тезах викладено інформацію щодо розробки мобільного застосунку, який значно полегшує опрацювання інформаційного простору між студентами, викладачами та підрозділами університету. Фреймворк Spring обрано для написання серверної частини додатку, залучено Spring Boot, Spring MVC та Spring Data.

Описано надійний захист додатку від несанкціонованого доступу, що забезпечує цілісність даних завдяки використанню модуля Spring Security, його засобів та підходів до застосування в застосунку на основі JWT токенів.

Почнемо з проблем, які стали нашою мотивацією для створення мобільного додатку для студентів.

1. Необхідність витрачати час в чергах до деканату за довідками.
2. Потреба в зручному й доступному розкладі.
3. Перегляд інформації про самого студента в рамках закладу.
4. Складнощі при виборі дисциплін в рамках навчального семестру.
5. Будь-яке коротке опитування або голосування вимагає від студента фізичної присутності в навчальному закладі.

Для забезпечення автентифікації користувача на стороні клієнта, тобто мобільного застосунку, необхідно надати студенту можливість підтвердити себе. Найпростіший спосіб – логін та пароль. Для університету чудовим логіном слугує пошта студента. Пароль повинен

бути згенерований з налаштуваннями надійності – від восьми символів; включати малі, великі літери, цифри та знаки тощо.

Проте при розробці додатку треба думати про зручність для користувача. Процедура входу до системи через постійне введення паролю та логіну є незручним. Зберігати логін і, тим паче, пароль на пристрої суворо забороняється. Все, що збережено на пристрої користувача, може бути викрадено вірусним ПЗ або недобросовісним програмістом.

Однією з найважливіших задач, які постали перед командою, було розробити надійний захист додатку від несанкціонованого доступу та забезпечити цілісність даних студентів. Було прийнято рішення використати Spring Security модуль, який надає засоби аутентифікації, авторизації та захисту від поширених атак на основі JWT токенів (рис. 1).

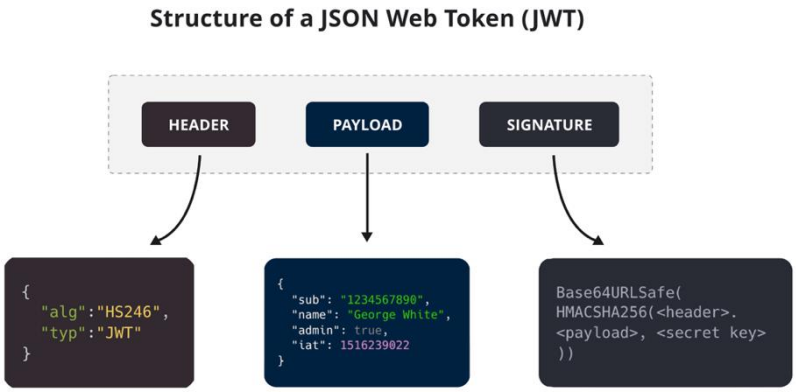

Рис. 1 - Структура JWT

Веб-токен JSON (JWT) — це відкритий стандарт (RFC 7519), який визначає компактний спосіб безпечної передачі інформації між сторонами, як об’єкт JSON. Цю інформацію можна перевірити та довіряти їй, оскільки вона має цифровий підпис. JWT можна підписати за допомогою секрету (з алгоритмом HMAC) або пари публічних та приватних ключів за допомогою RSA або ECDSA.

Підписані токени можуть підтвердити цілісність даних, що містяться в ньому, тоді як зашифровані токени приховують ці дані від інших сторін. Коли токени підписуються за допомогою пар публічних/приватних ключів, підпис також засвідчує, що лише сторона, яка володіє закритим ключем, є тією, яка його підписала.

Серверна частина мобільного додатку написана за допомогою фреймворка Spring. Він являє собою широкий набір модулів для розробки різних додатків. В нашому випадку було залучено Spring Boot, Spring MVC та Spring Data.

В нашому додатку токен підписується за допомогою HMAC алгоритму та секрету, який зберігається в конфігураційному файлі на сервері, що зводить до мінімуму можливість його викрадення, а отже і можливість розшифрувати токен зловмисником. В токені також зберігається ідентифікатор студента, за яким можна знайти необхідну інформацію про поточного студента у разі необхідності (рис. 2).

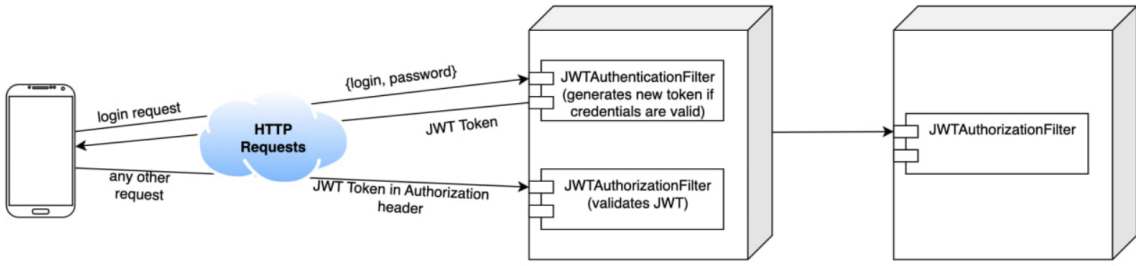

Рис. 2 – Алгоритм захисту інформації

До цього розробники часто використовували сесії для ідентифікації користувачів між різними запитами. Після введення коректних логіна та пароля, сервер генерував унікальний

ідентифікатор сесії, зберігав його в своїй пам'яті та відправляв на клієнт у вигляді кукі (від англ. Cookie). Цей ідентифікатор відправляється на сервер при запиті, порівнюється з тими, що вже зберігаються на сервері і, у разі знаходження, сервер надає доступ до ресурсу.

JWT являє собою новий підхід до авторизації користувача. На відміну від сесій, токени не зберігаються на сервері, можуть містити певну інформацію про користувача, а також не можуть бути підроблені без відповідного ключа.

Крім того, підхід з сесіями не є зручним для використання в мобільних додатках, так як вони не підтримують відправку інформації в куках. Токени ж можна легко передавати між сторонами та зберігати на мобільному застосунку в локальному сховищі.

Одним зі слабких місць даної технології є шанс викрадення токена у користувача. Пом'якшити наслідки від цього можна встановивши не дуже довгий період життя токена, протягом якого він вважається дійсним.

Отже, у ході розробки були виконані поставлені завдання та вирішені деякі проблеми взаємодії студентів та структур університету. В результаті ми отримали систему, здатну, забезпечити надійність та цілісність даних, відсіювати зловмисні запити і пропускати лише ті, які відправив власник даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. JWT [Електронний ресурс] – Режим доступу до ресурсу: https://jwt.io/introduction

2. Spring Security [Електронний ресурс] – Режим доступу до ресурсу: https://docs.spring.io/spring-security/reference/index.html

3. RSA Encryption Algorithm [Електронний ресурс] – https://www.javatpoint.com/rsa-encryption-algorithm

УДК 004.056.53

ЗАХИСТ ДАНИХ ТА ВИХІДНИХ ФАЙЛІВ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ТА КОПІЮВАННЯ КОМП'ЮТЕРНИХ ВІДЕОІГОР

ШАПОВАЛ В.В. (volodymyr.sh.05@gmail.com)
Київський національний університет імені Тараса Шевченка

У 21 столітті значних обертів набирає розвиток захисту даних інформаційних систем від злому та проникнення в систему. Однак, розвиток захисту від копіювання відеоігор стоїть на місці. Для опису проблематики було обрано декілька сучасних ігор, що були випущені на ринок протягом останніх 2-3 років. У доповіді було запропоновано перелік варіантів якісного та довгострокового вирішення цієї проблеми.

За останні десятиліття стрімких обертів набирає розробка відеоігор для різних платформ, як: ПК(Windows, Linux, MacOS), ігрові приставки(PlayStation, Xbox, Nintendo Switch), смартфони(Android, iOS) та планшети(Android, iPadOS). Незалежно від того, під яку платформу створюється відеогра, важливу роль відіграє захист файлів гри від злому чи копіювання. Наразі досягнути бажаного результату вдається лише ігровим приставкам. А все тому, що у наш час розвиток способів злому ігор, створення чіт-кодів чи копіювання ігор в цілому дійшло до такої грані, що багато провідних ігрових компаній світу не мають можливості та ресурсів з цим боротися.

Щоб навести приклади копіювання відеоігор та опублікування їх у просторах інтернету, оберемо три відеогри від трьох провідних компаній світу, що створюють якісний та популярний продукт. Перш за все, візьмемо до уваги гру «S.T.A.L.K.E.R.: Поклик Прип'яті» із серії «S.T.A.L.K.E.R.» компанії GSC Game World. Ця гра вийшла ще у далекому 2009 році. Однак вже за перші декілька місяців після релізу на просторах інтернету з'явилася