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.

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

велика кількість торент-файлів для завантаження гри безкоштовно. Можна подумати, що це було давно, а зараз так легко зробити копію гри вже не вдасться. Це буде хибна думка. Вже зараз, коли компанія планує випустити нову гру «S.T.A.L.K.E.R.: Серце Чорнобиля», на сайтах, де публікуються всі незаконно скопійовані ігри, є вкладка з цією грою. Це означає, що правопорушники вже напоготові до створення копії гри.

Тепер пропонуємо розглянути гру «Battlefield V» компанії Electronic Arts. Ця гра має декілька розділів: кампанія та багатокористувацька гра. Якщо пошукати в інтернеті способи, як завантажити цю гру безкоштовно, то можна побачити безліч робочих методів, але всі вони є лише частково робочими. Кампанія, або іншими словами одиночна гра, буде працювати навіть, якщо цю гру було незаконно скопійовано. А от багатокористувацька гра – ні, оскільки звичайного доступу до інтернету тут вже замало. Для того, щоб могти грати онлайн з іншими гравцями, потрібно мати акаунт в Origin. Якщо на вашому акаунті немає інформації про купівлю ліцензійної версії цієї гри, ви не зможете приєднатися до офіційних серверів, а отже, не матимете можливості грати онлайн.

І остання гра, яку ми взяли для проведення дослідження, - це «HALO 5: Guardians» компанії 343 Industries. Особливість цієї гри полягає в тому, що вона створена ексклюзивно для серії ігрових приставок Xbox компанії Microsoft. Придбати цю гру можна у вигляді диску або онлайн через офіційний магазин Microsoft Store. Завантажити копію цієї гри не можливо, оскільки її не існує. Але чому не можливо створити копію гри для ігрових приставок? Цьому є пояснення.

Жодна компанія, що створила операційну систему, не отримує відсотки з продажу ігор. У них немає фінансового інтересу, саме тому про захист від несанкціонованого доступу чи копіювання повинні думати платформи для купівлі ігор, як Steam, Origin, EA App, Uplay тощо. Однак, якщо поглянути на версії відеоігор, які створені саме для ігрових консолей, то можемо помітити, що придбати або завантажити копію гри неможливо. А все тому, що розробники Xbox, PlayStation чи Nintendo Switch мають фінансовий та рейтинговий інтерес. Якщо ігри для консолей середній статистичний гравець купує декілька разів на місяць, то саму ігрову приставку лише раз. Якщо дозволити користувачам копіювати відеоігри для консолей, це фактично означає позбавити себе можливості продавати ліцензійні версії ігор. Як результат, компанія-розробник приставки збанкрутує. Саме тому захистом від несанкціонованого доступу чи копіювання займається не лише компанія-розробник відеогри, а також компанія-розробник приставки.

І остання проблема, якій, на сьогоднішній день, приділяється мало уваги, - це нестача професійних кадрів у сфері управління, обробки та захисту інформації. Це відбувається через порівняно малу кількість вакансій в даній сфері. Саме тому майбутні студенти обирають спеціальності, випускники яких матимуть більшу конкурентоспроможність. В нашій країні мала частка компаній, що займаються захистом даних. Через це вітчизняні компанії звертаються з питань захисту до провідних компаній Європи. Також нестача вакансій у даній сфері призводить до відпливу талановитих людей. Найкращих працівників запрошують на роботу за кордоном. Але ні країні, ні ІТ-компаніям не вигідно втрачати таких спеціалістів.

Визначивши проблеми в захисті даних та вихідних файлів комп’ютерних відеоігор, пропонуємо усунути вище описані проблеми декількома способами:

- створити для кожної відеогри, незалежно від режиму гри (одиночна чи багатокористувацька), зв’язок із сервером та ігровою платформою, щоб жодна гра не могла бути запущена без авторизації ігрового акаунту та перевірки наявності придбаної ліцензійної версії гри із сервером;

- залучити до захисту даних та вихідних файлів компанії-розробників операційних систем. Таким чином система не буде такою вразливою до доступу до вихідних файлів;

- підвищити інтерес студентів до опанування навиків в управлінні, обробці та захисті інформації. У наш час майбутнім абітурієнтам потрібно створювати всі умови для обрання спеціалізації саме у сфері захисту інформації. Саме тому вже подана пропозиція про створення додаткової спеціалізації «Захист програм і даних» на спеціальності 121 «Інженерія

програмного забезпечення». Впевнені, що прийняття подібного рішення в багатьох ВНЗ України призведе до збільшення кількості якісних спеціалістів у даній сфері.

Як висновок, хочемо зазначити, що наші пропозиції можуть усунути не всі проблеми, що пов'язані із захистом даних та вихідних файлів комп'ютерних відеоігор, однак реалізація наших пропозицій може значно зменшити рівень копіювання відеоігор, порушення авторських прав, створення чіт-кодів чи іншого шкідливого забезпечення, що порушує умови компанії-розробника відеоігор та користувачів загалом.

УДК 004.056.5:004.738.5

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ РЕЗЕРВНОГО АРХІВУВАННЯ ДАНИХ У ХМАРНИХ СИСТЕМАХ

ШЕВЧУК Р.П. (rsh@wunu.edu.ua), **ЗАРІЦЬКИЙ О.І.** (olekszaritski@gmail.com)
Західноукраїнський національний університет

У роботі проведено аналіз існуючих хмарних систем резервного копіювання даних та запропоновано програмне забезпечення для забезпечення безпеки резервного архівування даних. Архітектура розробленого програмного забезпечення складається з шести основних модулів, які забезпечують безперебійну роботу системи резервного копіювання та мінімізують ризики викрадення архівних даних за рахунок покращення контролю доступу до них.

Вступ. Резервне архівування даних є важливою складовою забезпечення безпеки даних, та незамінним інструментом для забезпечення їх відновлення у випадку втрати [1]. Однак, при зберіганні даних в хмарі, існують додаткові ризики безпеки, такі як втрата даних внаслідок відмови обладнання, неправильної конфігурації, несанкціонованих доступ до даних, а також кібератаки [2,3]. Одним із підходів для зменшення цих ризиків є використання надійного програмного забезпечення для резервного архівування даних.

Мета роботи. Метою даної роботи є розробка програмного забезпечення для забезпечення безпеки резервного архівування даних у хмарних системах, яке дозволить мінімізують ризики викрадення архівних даних.

Основна частина. У роботі проведено аналіз існуючих систем резервного копіювання, зокрема: Amazon Web Services (AWS) Backup, Microsoft Azure Backup, Google Cloud Storage, Backblaze, Dropbox, Acronis Cloud Backup, IDrive Cloud Backup. За результатами аналізу описано технічні можливості та функціонал систем, виділено їх переваги та недоліки, а також оцінено ефективність їх роботи. Показано, що проаналізовані системи не враховують ряд ризиків, пов'язаних з використанням резервного архівування даних у хмарі.

Для зменшення цих ризиків у роботі розроблено спеціалізоване програмного забезпечення резервного архівування даних, яке дозволяє мінімізувати ризики викрадення архівних даних. Для розробки програмного забезпечення використано мови програмування C#, фреймворк ASP.Net та базу даних PostgreSQL.

Архітектура розробленого програмного забезпечення складається з наступних модулів: бази даних, черги розподілу завдань, вузлів обробки, модуля зберігання метаданих файлів, об'єктного сховища та планувальника резервного копіювання (рисунок 1).

У програмному забезпеченні для ідентифікації користувачів, контролю доступу та шифрування даних використано протокол Kerberos [4], а для авторизації сторонніх додатків для доступу до архівних даних протокол OAuth [5]. Використання цих протоколів дозволило забезпечити безпеку даних у хмарних сервісах, зменшити ризики викрадення даних та збільшити контроль за доступом до даних.