УДК 004.415.25

Мусянович О.В., Морозов Ю.В.

Національний університет "Львівська політехніка"

кафедра електронних обчислювальних машин

**ПІДСИСТЕМА ЗАХИСТУ МУЛЬТИМЕДІЙНОЇ ІНФОРМАЦІЇ НА ВЕБ-САЙТІ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ ВІРТУАЛЬНИХ ДИСКІВ**

*© Мусянович О.В., Морозов Ю.В., 2019*

**Розглянуто проблему захисту мультимедійної інформації, розглянуто способи захисту інформації, розроблено структурну схему системи та алгоритм її роботи.**

**Ключові слова:захист, шифрування, віртуальний диск, VeraCrypt, DRM.**

**MULTIMEDIA INFORMATION SECURITY SUBSYSTEM ON WEB SITE USING VIRTUAL DISC TECHNOLOGY**

*© Musyanovych O.M., MorozovY.V., 2019*

**The problem of protection of multimedia information and the ways of information protection are considered, the structural scheme of the system and the algorithm of its work are presented.**

**Keywords: protection, encryption, virtual disk, VeraCrypt, DRM.**

**Вступ**

Завдяки безперервному розвитку технологій, поширеність кібератак постійно зростає, а відстояти право власності стає все важче, оскільки за «піратство» не завжди і не всюди несуть хоч якусь відповідальність. Все частіше розробники программного забезпечення намагаються створити та вдосконалити різного роду DRM-системи щоб запобігти використанню інформації, або щоб притягти до відповідальності зловмисників, які порушують авторські права. Найширше технології DRM використовуються в індустрії розваг (кіноіндустрія та звукозапис)[6].

Хорошим прикладом засобів захисту мультимедіа є системи, які використовуються в Blu-ray дисках. Дані системи складаються як з апаратного захисту, так і з програмного. Файли, що записуються на диск, зашифровуються за допомогою динамічної системи шифрування, яку можна змінити, після того як вона була скомпроментована. Апаратна частина, в свою чергу, захищає він копіювання та відтворення неліцензійного контенту [7]. Такий же принцип роботи можна застосувати для створення та відтворення мультимедійних файлів, оскільки, як показує практика, зазвичай, системи з комбінованим захистом більш надійніші ніж з одинарним.

**Стан проблеми**

В мережі Інтернет, фактично, будь-яку інформацію можна завантажити та відтворити. Файли зазвичай зберігаються і передаються в незахищеному вигляді, в результаті чого виникає проблема захисту авторських прав при несанкціонованому розповсюдженні та відтворенні даного контенту. Обмеження доступу до файлу не вирішує проблеми його розповсюдження. Якщо файл не захищено – контролювати його розповсюдження практично неможливо. Захист файлу за допомогою паролю також не є достатньою мірою захисту, оскільки пароль можна також розповсюдити, і після цього видалити його повністю.

Щоб запобігти несанкціонованому відтворенню інформації, необхідно використати відтворювач, який виконуватиме перевірку доступу при відтворенні. Виконувати ручне завантаження файлів і розшифровування його за допомогою певної програми. користувачу вкрай незручно виникає потреба у відтворенні мультимедійних файлів з певного захищеного середовища. Таким середовищем можуть виступати віртуальні диски. Дані диски можуть певний зашифрований розділ, в якому всі дані будуть захищені, а можуть бути повністю «відкритими». В даному випадку він не є зашифрованим, і доступ до його вмісту надається користувачам системи. Для посилення захисту, можна закодувати файли, включивши в них так звану «сіль». Тому, при реалізації такої системи захисту, за бажанням, можна подбати як про шифрування диску загалом так і шифрування файлів безпосередньо. Але дане рішення може суттєво вплинути на швидкість роботи з великими файлами.

**Постановка задачі**

Розробити підсистему для захисту та відтворення мультимедійних файлів, яка складатиметься з програми-шифратора контенту, програми-дешифратора контенту та веб-сервісу, який забезпечує: обмін ключами між користувачами, зберігання зашифрованих файлів та контролю доступу до них.Розробити структурну схему та описати алгоритм роботи підсистеми загалом і кожної частини зокрема.

**Розв’язання задачі**

Для розв’язання даної задачі, було вирішено створити систему на базі клієнт-серверної архітектури. Клієнти – це клієнтські програми, які виконують шифрування, дешифрування та монтування віртуальних дисків, які містять певну мультимедійну інформацію. Для обмеження доступу та забезпечення шифрування мультимедійного контенту було вирішено використовувати технологію віртуальних дисків на базі VeraCrypt. Дана технологія дозволяє на льоту виконувати шифрування файлів та дисків та створювати віртуальні зашифровані диски [8]. Прямого доступу з файлової системи до файлів на зашифрованому диску не буде. Натомість, розробляється драйвер, який матиме можливість створити зашифрований диск з, поміщеними в нього, необхідними файлами та відтворення файлів з дешифруванням в режимі реального часу.

Для організації передачі файлів та доступу до них у вигляді ключів розробляється Веб-сервіс. Даний сервіс повинен забезпечувати коректне збереження дисків, передачу їх при запиті, авторизацію та автентифікацію користувачів сервісу. Веб-сервіс створюється засобами мови PHP з використанням бібліотеки Laravel Passport, яка має реалізовані методи авторизації та автентифікації.

Оскільки, диск буде зашифровано, щоб його розшифрувати, необхідні ключі. Протоколом обміну ключів було обрано протокол Diffie-Hellman, а для шифрування файлів віртуальних дисків було обрано PGP.Технологією розробки клієнтських аплікацій було обрано Xamarin.

Загальна структура системи матиме наступний вигляд:



Рис. 1 Структурна схема розроблюваної системи

На рисунку 1 наведено взаємодію між компонентами розроблюваної системи та блоки, з яких складається кожна з її частин. Веб-сервіс забезпечує взаємодію між створювачами та відтворювачами мультимедійного контенту через REST API-інтерфейс [2].

Для того щоб передати Веб-сервісу зашифровану інформацію її потрібно отримати з внутрішнього сховища або з камери. Користувачу достатньо обрати необхідні файли, які потрібно зашифрувати та передати, програма, в свою чергу, виконає всі необхідні маніпуляції з ними. Після завершення процедури шифрування віртуального диску, він надсилається на сервер, звідки його можна отримати, маючи необхідний доступ.

Щоб переглянути зашифровану інформацію необхідно авторизуватись і програма автоматично завантажить ключі, які необхідні для розшифрування файлу віртуального диску. Наступним кроком необхідно завантажити файл віртуального диску. Після того, як диск буде завантажено, розшифровано та змонтовано, користувачу будуть доступні необхідні файли в режимі читання.

Для реалізації програм шифрування та розшифрування мультимедійної інформації розроблено наступні алгоритми:



а) б)  
Рис. 2 а) програма шифрування мультимедійної інформації, б) програма дешифрування мультимедійної інформації

Приклад реалізації частини програми, яка працює з віртуальними контейнерами наведено на рисунку 3. В ньому наведено всі необхідні функції, які будуть реалізовані в вищевказаному драйвері.

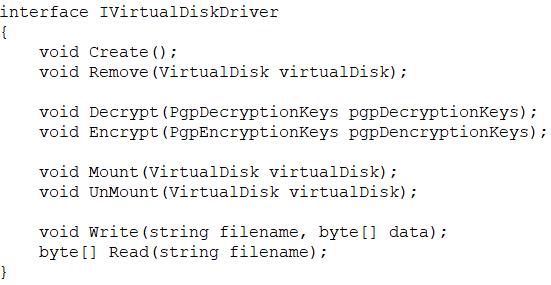


Рис. 3 Опис інтерфейсу драйвера для роботи з віртуальними дисками

**Висновки**

В роботі розроблено підсистему захисту мультимедійної інформації на Веб-сайті з використанням технології віртуальних дисків. Розроблювана система забезпечує створення, збереження та відтворення мультимедійної інформації. Також, в даній системі передбачена авторизація користувачів, та забезпечено обмін ключами між клієнтом і сервером. Розроблено структурну схему системи в цілому та описано алгоритми роботи клієнтських програм.

1. *Класифікація засобів модульної взаємодії між клієнтом і сервером / Ю. В. Морозов, І. І. Пастернак // Вісн. Нац. ун-ту "Львів. політехніка". - 2012. - № 717. - С. 108-112. - Бібліогр.: 10 назв. - укp;2. Мережні інтерфейси рівня клієнт-сервер / Ю. Морозов, І. Пастернак // Вісн. Нац. ун-ту "Львів. політехніка". - 2012. - № 743. - С. 121-130. - Бібліогр.: 16 назв. – укp; 3. О.З. Шологон Види загроз в кіберфізичних системах. - Львів :, 2015p; 4. Морозов Ю.В., Сокіл В.М. Цифрові сертифікати — основа системі дентифікації в комп’ютерних мережах // Вісник Національного університету «Львівська Політехніка»: «Комп’ютерні системи та мережі». 2002. — № 463. — C. 62–65; 5. В. О. Кононова, О. В. Харкянен, С. В. Грибков Оцінка засобів захисту інформаційних ресурсів. // Вісник Національного університету «Львівська Політехніка»: «Комп’ютерні системи та мережі» 2015р.; 6. Інтеграція права та інформатики: прикладний і змістовний аспекти : монографія / В. Г. Іванов, В. Ю. Шепітько, М. Г. Любарський та ін. ; за заг. ред. В. Г. Іванова, В. Ю. Шепітька, В. В. Карасюка. — Х. : Право, 2012. — 248 с.; 7. J. Lotspiech. “BroadcastEncryption”. MultimediaSecurity Technologies forDigitalRightsManagement, AcademicPress, Chapter 12, 2006; 8. Rubens, Paul (October 13, 2014). "VeraCrypt a WorthyTrueCryptAlternative". eSecurityPlanet. QuinstreetEnterprise. ArchivedfromtheoriginalonDecember 3, 2018. RetrievedFebruary 16, 2015.*