

ВИКОРИСТАННЯ УНІКАЛЬНИХ НЕЗМІННИХ ІДЕНТИФІКАТОРІВ ПРИСТРОЮ ДЛЯ ШИФРУВАННЯ ФАЙЛІВ

Вінницький національний технічний університет

Анотація

Розглянуто можливість використання незмінних унікальних ідентифікаторів пристрою для генерації ключів шифрування файлів. Досліджено переваги та важливість шифрування даних. Проаналізовано переваги та недоліки використання різних способів отримання ключів шифрування. Розглянуто доцільність використання унікальних незмінних ідентифікаторів пристрою для шифрування файлів.

Ключові слова: безпека, захист, файли, шифрування, ключі, користувацький досвід, зберігання, генерація, автоматизація, резервне копіювання.

Abstract

The possibility of using immutable unique device identifiers for generating file encryption keys is considered. The advantages and importance of data encryption are investigated. The advantages and disadvantages of using different methods of obtaining encryption keys are analyzed. The feasibility of using unique immutable device identifiers for file encryption is considered.

Keywords: security, protection, files, encryption, keys, user experience, storage, generation, automation, backup.

Вступ

Проблема безпеки даних та конфіденційності є надзвичайно актуальною у часи, коли більшість застосунків збирають різноманітні дані про користувача часто без його відома. Іноді це можуть бути некритичні дані, що використовуються для покращення застосунків, але також досить багато з них збирають дані своїх користувачів задля подальшого продажу або неетичного використання.

Причиною викрадення даних може стати власна необережність користувачів. Хоча більшість застосунків користувачі завантажують з офіційних платформ типу Play Store, де кожен застосунок проходить перевірку, проте не можна виключати можливості помилок у перевірці, а також можливості використання з першого погляду безпечних інструментів у зловмисних цілях. Навіть не дивлячись на це – завантаження з даних платформ застосунків всеодно є досить безпечним способом отримання програмних продуктів, проте багато людей можуть не знайти «найкращого» застосунку до своїх вимог серед них, звертаючись до сторонніх сайтів, де ризик натрапити на небезпечні для конфіденційності користувача файли значно зростає.

Завантаживши неперевірений файл із сумнівного джерела, недосвідчений користувач може несвідомо власними руками дати згоду для доступу до файлів пристрою, що дозволить зловмиснику викрасти усі файли даних із фотографіями та можливо нотаток з важливою інформацією.

Хоча захистити користувача від власної необережності можливо, це призведе до обмежень, які значно погіршать користувацький досвід. Відповідно кращим варіантом, що не буде погіршувати задоволення від користування пристроєм є захист самих даних від зловмисника.

Захист даних від викрадення зловмисниками

Для захисту пристрою від різноманітних загроз існують багато засобів та застосунків, таких як антивірусні програми, шифрування, блокування екрану, вбудовані механізми захисту в ОС та інші, проте лише декілька з них захищають пристрій від зловмисних застосунків, що були завантажені власне користувачем та наділені необхідними їм правами [1]. Найефективнішим з них є метод шифрування даних, адже він працює за іншим принципом ніж інші методи. Шифрування даних є унікальним тим, що замість блокування спроб викрасти дані – він забезпечує те, що викрадені дані буде неможливо відтворити неавторизованому користувачу, а отже такі дані не будуть доступні зловмиснику. Недоліком ж такого способу є те, що дані можуть бути знищені взагалі, проте просте їх дублювання або створення резервної копії попередить їх втрату [2].

Зберігання ключів шифрування та ризики

Для шифрування та дешифрування використовуються так звані ключі шифрування – криптографічні параметри, що використовуються у алгоритмах шифрування для унікальності шифрування даних, у симетричних алгоритмах ключі для шифрування та дешифрування співпадають, в той час як у асиметричних – різняться. Не знаючи ключів шифрування розшифрувати дані є майже непосильною задачею, що робить їх зберігання надзвичайно важливою задачею, адже якщо зломисник отримає дані ключі – шифрування не матиме сенсу [2].

Для зберігання ключів шифрування існує декілька способів, серед них:

- апаратні засоби безпеки (HSM). Це спеціалізовані апаратні пристрої, призначені для безпечного зберігання та обробки криптографічних ключів. Вони забезпечують високий рівень захисту від несанкціонованого доступу та фізичної крадіжки ключів;

- токени безпеки. Це фізичні пристрої, які зберігають ключі шифрування та можуть бути використані для аутентифікації та дешифрування даних. Токени безпеки часто використовуються для додаткової безпеки під час доступу до зашифрованих даних;

- хмарні рішення. Деякі хмарні сервіси пропонують керування ключами шифрування, де ключі зберігаються на серверах постачальника, але можуть бути керовані клієнтом за допомогою керованих клієнтом ключів (CMK);

- зберігання у файлах або у пам'яті. Ключі можуть зберігатися у файлах або базах даних, але це вимагає додаткових заходів безпеки для захисту цих носіїв інформації.

Хоча ці способи і є популярними, проте для рядового користувача вони можуть бути занадто вимогливими, незручними або недостатньо надійними, іншим варіантом отримання ключів шифрування є постійна генерація ключів, досить часто різні застосунки генерують ключі шифрування на основі паролів або інших персоналізованих засобах безпеки, що дозволяє взагалі не зберігати ключі шифрування, а відповідно й не мати ризику їх викрадення, проте це створює необхідність користувачу запам'ятовувати свій пароль, що створює ризик втрати даних при забутті паролю [3].

Іншим способом генерації ключів є генерація ключів на основі певних незмінних унікальних параметрів, що не тільки отримає переваги генерації ключів на основі паролю користувача, але і звільнить користувача від необхідності запам'ятовування паролю.

Переваги та недоліки генерації ключів шифрування на основі незмінних даних пристрою

Генерація ключів на основі незмінних даних пристрою має ряд переваг, серед яких:

- надійне приховування ключів шифрування через відсутність потреби у їх зберіганні на пристрої;
- неможливість відтворення даних на інших пристроях без участі користувача;
- відсутність потреби у запам'ятовуванні будь-яких паролів з боку користувача, що спрощує процес шифрування та покращує досвід використання;
- неможливість до пристрою та відсутність потреби у додаткових витратах з боку користувача для додаткових пристроїв.

Даний спосіб не є ідеальним та має певні недоліки, наприклад:

- неможливість відновлення даних при зміні або втраті пристрою;
- ризик дублювання унікальних даних. Якщо зломиснику вдасться здублювати унікальні параметри пристрою на несертифікованому пристрої, він зможе отримати доступ до даних.

Способи вирішення проблем шифрування з генерацією ключів

Такий ризик як дублювання унікальних даних на несертифікованому пристрої досить важко, якщо не неможливо усунути без значних поступок у перевагах або створенні нових недоліків. Проте недолік відновлення даних на іншому пристрої можливо усунути повністю з невеликими поступками у зручності використання. Для цього можна використати 2 методи:

1. Зняття шифрування перед пересиланням даних між пристроями. Даний метод є найбільш очевидним та простим, проте це створює великий ризик викрадення даних при пересилці, що є значною прогалиною у безпеці даних.

2. Подвійне шифрування при створенні резервної копії даних. Даний спосіб передбачає збереження файлу резервного копіювання разом з вставленим у ньому згенерованим ключем шифрування, після чого даний файл шифрується другий раз, але на цей раз з ключем, що згенерований на основі пароля користувача. Таким чином залишається надійність зберігання даних, при цьому не маючи великого ризику забуття паролю, адже операція резервного копіювання та відновлення не передбачає довгих строків, у той же час якщо користувач буде зберігати даний файл копії паралельно з основним – це знизить ризик втрати даних через забуття паролю, адже основні дані все ще збережені на основному пристрої з автоматичним ключем і можуть бути зарезервовані повторно.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Способи захисту пристрою від атак [Електронний ресурс] – режим доступу до ресурсу: <https://datami.ee/ua/blog/bezpeka-i-kiberbezpeka-smartfoniv/>.
2. Переваги шифрування [Електронний ресурс] – режим доступу до ресурсу <https://www.ibm.com/think/topics/encryption>.
3. Менеджмент ключів шифрування [Електронний ресурс] – режим доступу до ресурсу: <https://research.aimultiple.com/encryption-key-management/>.

Кучеренко Максим Володимирович – студент групи 1ПІ-24м кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця, e-mail: eliksplay@gmail.com

Майданюк Володимир Павлович – канд. техн. наук, доцент кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця, e-mail: maidaniuk2000@gmail.com.

Kucherenko Maksym Volodymyrovych – student of group 1PI-24m of the Department of Software, Vinnytsia National Technical University, Vinnytsia, e-mail: eliksplay@gmail.com.

Maidaniuk Volodymyr Pavlovych – candidate of technical sciences, associate professor of the Department of Software, Vinnytsia National Technical University, Vinnytsia, e-mail: maidaniuk2000@gmail.com.