DOI 10.15276/imms.v14.no3.172
УДК 004.056.53

Informatics and Mathematical Methods in Simulation
Vol.14 (2024), No. 3, pp. 172-182

ЗАСТОСУВАННЯ ОБФУСКАЦІЇ ДЛЯ ЗАХИСТУ МЕТАДАНИХ ФАЙЛІВ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Є.С. Булгаков, Н.І. Кушніренко, В.В. Подуфалов, В.О. Назаров

Національний університет «Одеська політехніка»
1, Шевченка пр., Одеса, 65044, Україна
Email: infsec2011@gmail.com

Розглянуто проблему захисту метаданих файлів від несанкціонованого доступу за допомогою обфускації. Метадані відіграють ключову роль у сучасних цифрових системах, забезпечуючи важливу інформацію про файли, таку як авторство, дата створення, геолокація, тип пристрою та інші атрибути, що допомагають у їх ідентифікації та класифікації. Однак ці дані можуть стати вразливими для кібератак, оскільки зловмисники можуть використовувати метадані для збору конфіденційної інформації або здійснення атак на користувачів та організації. Детально проаналізовано різні методи обфускації метаданих, зокрема шифрування, маскування та фальсифікацію, кожен з яких має свої переваги і недоліки. Шифрування дозволяє забезпечити високий рівень захисту, однак вимагає управління ключами, що може бути складним для великих організацій. Маскування передбачає заміну реальних значень метаданих псевдонімами або випадковими значеннями, зберігаючи при цьому функціональність файлів. Фальсифікація метаданих полягає у створенні неправдивої інформації для введення зловмисників в оману. Окрім того, у статті запропоновано концепцію розробки спеціалізованого програмного забезпечення для автоматизованого захисту метаданих, яке дозволяє користувачам автоматично обфускувати або видаляти метадані файлів під час їх обробки чи передачі через мережу. Програмне забезпечення також включає можливість групової обробки файлів, що є важливим для організацій, які працюють із великими обсягами даних. Такі рішення є актуальними в умовах сучасних кіберзагроз, оскільки забезпечують високий рівень конфіденційності та захисту даних. Важливим аспектом є те, що запропоноване програмне забезпечення не лише обфускує дані, але й інтегрується з іншими системами для автоматизації процесів захисту.

Таким чином, у роботі підкреслено важливість застосування обфускації як інструменту для підвищення рівня інформаційної безпеки та захисту конфіденційної інформації. Запропоноване програмне рішення є перспективним кроком у вирішенні проблеми витоків даних через метадані та може знайти застосування у різних галузях, включаючи медицину, освіту, архітектуру, геймдев, де захист даних відіграє ключову роль.

Ключові слова: захист метаданих, обфускація, шифрування, маскування, фальсифікація, програмне забезпечення.

Вступ. У сучасному світі інформаційні технології стають дедалі важливішими в усіх сферах людської діяльності, що призводить до безпрецедентного зростання обсягів даних, які передаються, зберігаються та обробляються. Відомі випадки, коли вразливість метаданих призводила до значних фінансових втрат. Наприклад, в одному з кейсів компанія з Лондона втратила близько 500 000 доларів США через компрометацію конфіденційних метаданих їхніх файлів під час передачі через мережу [1]. В іншому дослідженні, проведеному в області захисту метаданих, було показано, що понад 80% конфіденційних документів, які зберігаються в хмарних системах, містять незахищені метадані, що може бути використано зловмисниками для атак [2]. Поряд із вмістом файлів, значну роль відіграють метадані — інформація про файли, яка використовується для забезпечення їх ідентифікації, класифікації, індексації та впорядкування. Метадані містять такі відомості, як ім'я автора, дата створення або редагування файлу, тип пристрою, на якому був створений файл, геолокація тощо. У багатьох випадках метадані

несуть не менш важливу, а іноді навіть критично важливу інформацію, яка може бути використана для отримання доступу до приватних або конфіденційних даних.

Однією з основних проблем, що виникають у зв'язку з використанням метаданих, є їхня вразливість до несанкціонованого доступу та використання. Наприклад, зловмисники можуть отримати доступ до метаданих документів або мультимедійних файлів, щоб виявити інформацію про автора, місцезнаходження або інші важливі дані, які не призначені для загального доступу. Це може призвести до порушення приватності, конфіденційності або навіть безпеки користувача.

Одним із ефективних способів захисту метаданих є застосування методу обфускації, який передбачає перетворення або приховування метаданих таким чином, щоб вони ставали нерозбірливими або недоступними для зловмисників. Обфускація метаданих дозволяє забезпечити конфіденційність інформації, що міститься у файлах, зберігаючи при цьому їхню функціональність для законних користувачів. Серед програмних рішень для обфускації можна виділити такі інструменти, як ExifTool та Metadata Anonymization Toolkit (MAT), які вже успішно застосовуються для захисту метаданих у великих корпораціях [3]. Проте вони мають свої недоліки, такі як недостатня автоматизація або повне видалення метаданих, що може знижувати зручність використання для кінцевих користувачів. Це створює потребу у нових, більш гнучких рішеннях, що можуть захистити метадані без втрати важливих функцій файлів [4].

Окремо варто звернути увагу на захист інтелектуальної власності у сфері 3D-моделювання, де метадані також відіграють важливу роль. Метадані 3D-файлів можуть містити інформацію про авторство, дати створення, використані інструменти та інші важливі атрибути, які допомагають ідентифікувати власників моделей та захищати їх права. Однак відсутність ефективного захисту цих даних може призвести до незаконного копіювання та використання 3D-моделей, що вже призводило до значних збитків у таких галузях, як кіноіндустрія та розробка відеоігор [5]. Наприклад, плагіни для захисту авторських прав, як-от плагін для Blender [6], дають можливість творчим професіоналам захищати свої роботи шляхом накладання водяних знаків на моделі та приховування важливих метаданих від несанкціонованого доступу.

В даній роботі розглядаються основні поняття, пов'язані з метаданими та їхнім захистом, обґрунтовується необхідність захисту метаданих, а також наводяться підходи до їхньої обфускації. Крім того, пропонується власне програмне забезпечення для обфускації метаданих у різних типах файлів з метою забезпечення їх захисту від несанкціонованого доступу.

Дана тема є актуальною через значний ріст обсягів даних і поширення інтернет-комунікацій, що супроводжується зростанням загроз у сфері інформаційної безпеки. Важливо зазначити, що сучасні користувачі часто не усвідомлюють, наскільки багато інформації про них може бути витягнуто через метадані, що робить їх потенційними мішенями для різного роду кіберзлочинців. Використання методів обфускації дозволяє мінімізувати ці ризики та забезпечити вищий рівень безпеки для особистої та корпоративної інформації.

Мета і задачі дослідження. Мета роботи розробці власного програмного забезпечення для захисту метаданних файлів різних типів за допомогою обфускації. Для досягнення цієї мети необхідно виконати наступні задачі:

1. Розглянути поняття метаданих та проаналізувати загрози, які можуть виникнути через несанкціонований доступ до них.
2. Розглянути існуючі методи обфускації та їх реалізацію на практиці, а також дослідити доцільність застосування обфускації до захисту метаданих файлів.
3. Запропонувати власне програмне забезпечення для обфускації метаданих з метою їх захисту.

Основна частина. Метадані — це структуровані дані, які надають додаткову інформацію про самі дані або файли. Їх основне призначення — полегшити пошук,

ідентифікацію, організацію і керування вмістом файлу чи об’єкта. Вони використовуються для забезпечення опису інформації, її класифікації, а також для управління файлами. Метадані супроводжують майже всі цифрові файли — від текстових документів до мультимедійних матеріалів, і навіть файлів баз даних або веб-сторінок.

Приклади метаданих включають:

- Документи: автор, дата створення, кількість сторінок, мова.
- Мультимедійні файли (фото, відео, аудіо): дозвіл зображення, тривалість відео, дата і місце зйомки, інформація про камеру, програмне забезпечення, яке використовувалось для редагування.
- Електронні листи: дата й час надсилання, отримувач, тема, IP-адреса відправника.
- Файли програмного коду: версія коду, автор, дата останнього редагування, список використаних бібліотек.

Метадані можуть бути не лише видимими частинами файлів, але й прихованими даними, які автоматично створюються операційними системами або програмами під час обробки, збереження чи пересилання файлів. Ця прихована інформація може бути важливою для користувачів, але в деяких випадках може бути використана зловмисниками для несанкціонованого доступу до конфіденційних даних.

Метадані є критичним елементом управління інформацією в будь-яких інформаційних системах. Вони виконують ряд важливих функцій:

1. Ідентифікація файлів та їхнього вмісту. Метадані дозволяють швидко зрозуміти, про що йдеться у файлі, без необхідності відкривати або переглядати його повний вміст. Наприклад, за допомогою метаданих можна отримати інформацію про автора документа, дату створення або редагування, і навіть мову, на якій він написаний.
2. Організація та управління даними. Метадані дозволяють структурувати інформацію та допомагають системам керування файлами індексувати й категоризувати їх. Це полегшує пошук файлів у великих системах даних, наприклад, у базах даних або медіа-архівах.
3. Пошук інформації. Метадані використовуються для забезпечення швидкого та ефективного пошуку потрібної інформації в інформаційних системах. Завдяки метаданим користувачі можуть легко фільтрувати документи за автором, датою або темою, що значно пришвидшує процес отримання потрібних даних.
4. Відстеження змін та версій документів. Метадані можуть зберігати інформацію про зміни, які вносилися в документи або файли, зокрема дату і час редагування, а також ім'я користувача, який вносив ці зміни. Це дозволяє ефективно відстежувати версії файлів і відновлювати їх до попередніх станів у разі потреби.

Попри свою корисність, метадані можуть нести певні загрози безпеці. Через невидимість та автоматичний характер створення, багато користувачів можуть навіть не підозрювати, що їхні файли містять метадані, що можуть розкрити важливу інформацію. Основні загрози включають:

1. Компрометація конфіденційної інформації. Метадані можуть містити інформацію, яка розкриває особисті або корпоративні дані, наприклад, місце зйомки фотографії або автора документа. Якщо ці дані потраплять у руки зловмисників, це може призвести до витоку конфіденційної інформації.
2. Сприяння фішинговим атакам. Аналізуючи метадані електронних листів або документів, зловмисники можуть створити спеціальні фішингові повідомлення, орієнтовані на конкретних осіб чи компанії. Метадані можуть містити ключову інформацію, яка використовується для створення правдоподібного листа від імені особи або організації, що врешті-решт підвищує шанси на успіх атаки.
3. Відстеження дій користувачів. Метадані можуть містити хронологічну інформацію про дії користувача, що дозволяє зловмисникам відстежувати активність

конкретної особи або компанії. Наприклад, метадані фотографій можуть містити дані про геолокацію, що дозволяє точно визначити місцезнаходження користувача на момент створення фото.

4. Інформаційна асиметрія. У ситуаціях, коли файли передаються або публікуються в інтернеті, особа, яка отримує ці файли, може мати доступ до значно більшого обсягу інформації про їхній вміст, ніж автор файлу, що призводить до ризику несанкціонованого використання цих даних.

Захист метаданих є важливим кроком у забезпеченні загальної інформаційної безпеки. Основні причини, чому варто звернути увагу на захист метаданих, включають:

- Конфіденційність. У багатьох випадках метадані містять особисті або чутливі дані, які можуть стати предметом інтересу зловмисників. Їхня компрометація може призвести до порушення конфіденційності користувача або організації.

- Запобігання несанкціонованому доступу. Захищені метадані зменшують можливість для зловмисників отримати доступ до інформації, яка може бути використана для здійснення атак, збору інформації про користувачів або проведення розвідувальних дій.

- Захист репутації. Витоки інформації через метадані можуть завдати значної шкоди репутації як окремим особам, так і компаніям. Уразливі метадані можуть розкрити інформацію про внутрішні процеси, технічні подробиці або навіть стратегії організацій, що може негативно вплинути на їхні стосунки з партнерами або клієнтами.

- Відповідність нормативним вимогам. У багатьох країнах існують нормативні акти, що регулюють обробку та зберігання персональних даних, включаючи метадані. Невиконання цих вимог може призвести до юридичних наслідків і штрафів.

Отже, захист метаданих є важливим елементом інформаційної безпеки, який дозволяє мінімізувати ризики витоку конфіденційної інформації та забезпечити захист особистих і корпоративних даних від несанкціонованого використання. У наступних розділах буде розглянуто, як метод обфускації може бути застосований для ефективного захисту метаданих.

Загрози безпеці метаданих. Метадані можуть містити чутливу інформацію, яку часто недооцінюють як користувачі, так і організації. Оскільки метадані автоматично створюються різними програмами та операційними системами, користувачі можуть навіть не знати про їх існування або важливість. Ця невидимість призводить до того, що метадані можуть стати легкою мішенню для кіберзлочинців або зловмисників, які використовують їх для збирання розвідувальної інформації або запуску атак. У цьому розділі розглянемо основні загрози, пов'язані з метаданими, та їхній вплив на безпеку.

1. Витік конфіденційної інформації

Метадані можуть містити важливу інформацію, яку можна використати для несанкціонованого доступу до системи або для ідентифікації осіб. Наприклад:

Інформація про автора файлу: якщо метадані файлу зберігають ім'я або ідентифікатор користувача, який створив або редагував файл, зловмисники можуть використовувати ці дані для збору інформації про певних осіб або організації.

Геолокація: фотографії або відео можуть містити географічні координати, що розкривають місцезнаходження користувача в момент зйомки. Це може бути використано для відстеження фізичних переміщень або для планування фішингових атак, орієнтованих на певне місце.

Інформація про пристрій або програмне забезпечення: метадані можуть містити дані про версію програмного забезпечення, операційну систему або тип пристрою, на якому було створено файл. Це може надати зловмисникам інформацію для планування атак, націлених на вразливості конкретного програмного забезпечення.

2. Полегшення фішингових атак

Метадані можуть полегшити проведення цілеспрямованих фішингових атак (спеар-фішинг), особливо якщо в них міститься інформація про службовців або

внутрішні процеси організації. Зловмисники можуть використовувати цю інформацію для створення персоналізованих листів або повідомлень, які видаються за офіційні комунікації від відомих відправників.

3. Відстеження дій користувачів

Метадані можуть також містити інформацію про дії користувачів і зміни, які відбувалися з файлом протягом його життєвого циклу. Це може включати дати створення і редагування, імена користувачів, які вносили зміни, а також інформацію про місце, де були створені файли.

Ці дані можуть бути використані для:

Моніторингу активності користувачів: аналізуючи метадані, зловмисники можуть простежити, хто і коли працював з певними файлами, а також як часто вносилися зміни. Це може дозволити їм зрозуміти внутрішні робочі процеси організації або особисті звички користувача.

Створення профілів користувачів: шляхом збирання метаданих з різних файлів можна скласти детальний профіль активності користувача, включаючи його поведінку, місцезнаходження і використані пристрої.

4. Використання метаданих для соціальної інженерії

Соціальна інженерія — це набір технік, спрямованих на маніпуляцію людьми з метою отримання доступу до конфіденційної інформації або систем. Метадані можуть слугувати важливим джерелом для збору інформації, яка потім використовується для соціальної інженерії. Зловмисники можуть скористатися метаданими для створення довіри, імітації офіційних документів або повідомлень, і таким чином підвищити шанси на успіх атаки.

Соціальна інженерія може включати.

Фальшиві документи: зловмисники можуть змінити метадані файлу, щоб створити вигляд, що цей документ походить від надійного джерела, навіть якщо він є підробкою.

Імітація службовців або організацій: за допомогою метаданих можна дізнатися імена або посади певних осіб в організації і використовувати цю інформацію для створення фальшивих листів або документів.

5. Юридичні та регуляторні наслідки

У деяких випадках витік або несанкціоноване використання метаданих може призвести до серйозних юридичних наслідків для компаній або організацій. Наприклад, відповідно до законів про захист даних, таких як Європейський Загальний регламент про захист даних (GDPR), компанії зобов'язані забезпечити належний захист особистої інформації, включаючи метадані. Якщо ці дані будуть розкриті або використані без згоди, це може призвести до штрафів або інших санкцій.

Організації, які не забезпечують належного захисту метаданих, можуть бути притягнуті до відповідальності за витоки інформації, що ставить під загрозу їхню репутацію і фінансову стабільність.

6. Інформаційна асиметрія

Зловмисники можуть використовувати метадані для створення інформаційної асиметрії, тобто ситуації, коли одна сторона володіє значно більшим обсягом інформації, ніж інша. У таких випадках метадані можуть використовуватися для отримання переваги в переговорах або для маніпуляцій.

Застосування обфускації для захисту метаданих. Обфускація — це процес свідомого ускладнення або приховування інформації з метою ускладнення її аналізу сторонніми особами. Вона використовується для того, щоб зробити дані важкодоступними або непридатними для аналізу, навіть якщо зловмисники отримають до них доступ. У сфері інформаційної безпеки обфускація застосовується для захисту різних видів даних, включаючи метадані, код програмного забезпечення, структуру баз даних і навіть мережевий трафік.

Процес обфускації полягає у навмисній зміні структури або змісту даних таким чином, щоб вони залишалися функціональними або придатними для використання, але водночас були важкими для розуміння або аналізу третіми особами. Для метаданих обфускація може включати:

- Шифрування ключових полів: шифрування або заміна особливо чутливих частин метаданих, таких як імена авторів, дати створення або геолокаційні дані, щоб ці поля залишалися непридатними для читання без відповідного ключа дешифрування.
- Заміна дійсних даних на псевдоніми: використання псевдонімів або випадкових значень замість реальних імен чи інших ідентифікаторів. Наприклад, імена авторів документів можуть бути замінені на випадкові рядки символів або псевдоніми, що не мають жодного зв'язку з реальними людьми.
- Створення фальшивих метаданих: створення "пасток" для зловмисників у вигляді фальшивих метаданих, що вводять їх в оману або заплутують під час спроб аналізу файлів. Це можуть бути випадкові або хибні дані, що виглядають правдоподібно, але не мають жодного відношення до реальних файлів.
- Ускладнення структури даних: зміна структури або формату метаданих, наприклад, шляхом додавання випадкових символів або змішування значень полів, що ускладнює розуміння їхньої реальної суті без попереднього аналізу.

Обфускація метаданих надає кілька суттєвих переваг для забезпечення їхньої безпеки:

- Захист конфіденційної інформації. Обфускація дозволяє захистити особисту або чутливу інформацію, зберігаючи функціональність файлів, але приховуючи важливі деталі, які можуть бути використані зловмисниками.
- Запобігання зворотному інжинірингу. Зловмисники часто використовують аналіз метаданих для зворотного інжинірингу (відновлення початкових даних або отримання розвідувальної інформації). Обфускація значно ускладнює цей процес, оскільки спотворені або приховані дані важко відновити.
- Складність аналізу даних. Навіть якщо зловмисники отримають доступ до метаданих, обфускація робить їх малозрозумілими та не придатними для аналізу, оскільки маскує важливі елементи інформації.
- Захист від автоматизованих атак. Багато атак на метадані здійснюються за допомогою автоматизованих інструментів, які аналізують вміст файлів. Обфускація метаданих значно знижує ефективність таких інструментів, оскільки приховує або спотворює ключові дані, що використовуються для атак.

Серед методів обфускації, що застосовуються до метаданих, можна виділити кілька основних підходів:

1. Шифрування метаданих

Шифрування є одним із найефективніших методів захисту метаданих. Використовуючи симетричне або асиметричне шифрування, можна закрити доступ до чутливих полів метаданих, таких як імена, дати, місця зйомок тощо. Тільки ті користувачі, які мають відповідний ключ дешифрування, можуть прочитати ці дані.

Перевагою цього методу є високий рівень захисту, оскільки шифровані дані практично неможливо прочитати або змінити без ключа. Проте недоліком є необхідність керування ключами, що може ускладнити роботу для кінцевих користувачів, особливо в великих організаціях.

2. Маскування даних

Маскування полягає у заміні реальних значень метаданих випадковими або псевдонімними значеннями. Наприклад, імена авторів можуть бути замінені на послідовність випадкових символів або на нейтральні значення. Це дозволяє зберегти роботу з файлами без розкриття реальних ідентифікаторів.

Маскування є зручним для ситуацій, коли шифрування надто складне або недоцільне. Проте цей метод може бути менш ефективним у випадках, коли зловмисники

можуть інтуїтивно здогадатися про справжнє значення замаскованих даних на основі контексту.

3. Видалення метаданих

Один із найпростіших методів захисту — повне видалення метаданих з файлів перед їхнім передаванням або публікацією. Хоча це ефективно усуває ризик витоку інформації через метадані, цей метод може позбавити користувачів корисної інформації, яка може бути потрібна для організації або ідентифікації файлів.

Видалення метаданих підходить для випадків, коли метадані не є критично важливими для подальшого використання файлу. Однак цей метод не є прийнятним у тих ситуаціях, де метадані грають ключову роль (наприклад, у роботі з науковими статтями або іншими документами, де важлива інформація про автора).

4. Фальсифікація метаданих

Цей метод полягає у внесенні неправдивих або фальшивих даних у метадані, щоб ввести в оману потенційних зловмисників. Наприклад, можна вставити неправдиві імена, дати або геолокаційні дані. Така стратегія створює інформаційні "пастки", які роблять процес аналізу складнішим і менш надійним.

Фальсифікація метаданих добре підходить для випадків, коли потрібно замаскувати реальні дані, але при цьому важливо, щоб файл виглядав автентично для зловмисника. Проте цей метод може виявитися складним для реалізації на великих обсягах файлів.

Хоча обфускація є потужним інструментом для захисту метаданих, вона має певні обмеження:

- Неможливість абсолютного захисту. Як і будь-який інший метод захисту, обфускація не гарантує абсолютної безпеки. Досвідчені зловмисники можуть використовувати спеціалізовані інструменти для відновлення або аналізу обфускованих даних, хоча це значно ускладнює їхню роботу.
- Складність у використанні. Деякі методи обфускації, наприклад, шифрування або фальсифікація метаданих, можуть вимагати додаткових ресурсів або знань для налаштування й підтримки, що може бути складним для великих організацій або некваліфікованих користувачів.
- Зниження функціональності. Оскільки обфускація може змінювати або приховувати метадані, це може призвести до зниження функціональності файлів або до труднощів в їхньому використанні для деяких операцій (наприклад, для пошуку або каталогізації документів).

Таким чином, обфускація є одним із найефективніших і гнучких методів захисту метаданих, що допомагає забезпечити конфіденційність та безпеку інформації. Її використання дозволяє значно ускладнити доступ до важливих даних для зловмисників, одночасно забезпечуючи можливість роботи з файлами для авторизованих користувачів. Проте для досягнення максимальної ефективності її слід застосовувати в поєднанні з іншими методами захисту, зокрема шифруванням і управлінням доступом до файлів.

Практичні методи застосування обфускації для захисту метаданих. З огляду на теоретичні основи обфускації та її переваги, цей розділ присвячено практичним методам застосування обфускації для захисту метаданих у реальних сценаріях. Ми розглянемо конкретні способи, якими можна захистити метадані файлів, використовуючи різні інструменти та підходи, а також запропонуємо концепцію програмного забезпечення, яке можна розробити для автоматизації цього процесу.

У сучасному світі існують кілька інструментів і методів, які можуть бути використані для захисту метаданих шляхом їх обфускації або видалення. Ось кілька прикладів:

- ExifTool — це популярний інструмент для редагування, видалення і перегляду метаданих у файлах різних форматів (фотографії, відео, документи тощо). Він дозволяє змінювати або видаляти метадані, такі як геолокація, авторство, дата створення і

редагування тощо. Цей інструмент можна використовувати для обфускації шляхом видалення чутливих даних або їх заміни на хибні.

- Metadata Anonymization Toolkit (MAT) — це набір інструментів для видалення метаданих з різних типів файлів. Він забезпечує повну анонімізацію файлів шляхом видалення метаданих без зміни вмісту самого файлу. MAT є корисним у ситуаціях, коли потрібен швидкий і простий спосіб захисту інформації, однак він не використовує методи обфускації, оскільки повністю видаляє метадані.
- PyExifTool — це бібліотека Python для роботи з метаданими через ExifTool. Вона дозволяє програмно керувати метаданими з метою їх обфускації або видалення. Використовуючи PyExifTool, розробники можуть створювати власні сценарії для обфускації даних, включаючи маскування, фальсифікацію або шифрування чутливих елементів.

Ручне керування метаданими за допомогою інструментів на кшталт ExifTool або MAT може бути складним і вимагати багато часу, особливо при роботі з великими обсягами файлів. Тому корисним є створення автоматизованих систем для обфускації метаданих, які б працювали без участі користувача або з мінімальним втручанням. Нижче описані кілька можливих підходів для автоматизації обфускації.

1. Інтеграція обфускації у файлові системи

Одним із рішень для автоматизації процесу обфускації є інтеграція відповідних функцій у файлові системи або системи управління документами. Наприклад, можна створити систему, яка автоматично обфускує або видаляє метадані файлів під час їхнього завантаження або передачі через мережу. Це може бути корисним для організацій, які працюють із конфіденційними даними та хочуть захистити інформацію на рівні корпоративних процесів.

2. Використання API для обфускації

Ще одним підходом є створення API для обфускації метаданих, яке можна інтегрувати у програмне забезпечення для редагування або обробки файлів. API може виконувати операції з метаданими на хмарних сервісах або у локальних системах, дозволяючи автоматизовано замінювати, шифрувати або видаляти метадані перед збереженням або публікацією файлів.

3. Обфускація під час передачі файлів

Під час передачі файлів через мережу, особливо в рамках публічних систем або служб обміну файлами, доцільно впровадити механізми автоматичної обфускації. Перед тим, як файл передається до одержувача, система може здійснювати обфускацію його метаданих, залишаючи оригінальні метадані тільки у відправника. Це дозволить зберегти конфіденційність без втрати важливих даних для внутрішнього використання.

Програмне забезпечення для захисту метаданих з застосуванням обфускації. Пропонується концепція спеціалізованого програмного забезпечення для захисту метаданих, яке використовувало б методи обфускації, шифрування та видалення метаданих для забезпечення безпеки.

1. Функціонал програмного забезпечення

Програмне забезпечення для захисту метаданих містить такі ключові функції:

Аналіз метаданих: система повинна вміти сканувати файли та визначати наявні метадані. Це дозволить користувачам бачити, яку саме інформацію містить файл і які поля можуть бути вразливими до атак.

Обфускація метаданих: система дозволить користувачам автоматично обфускувати метадані, вибираючи між шифруванням, маскуванням або фальсифікацією даних.

Видалення метаданих: програмне забезпечення повинно також мати функцію повного видалення метаданих із файлів для випадків, коли немає потреби у їх збереженні.

Групова обробка файлів: для організацій, які працюють із великими обсягами даних, важливою функцією буде можливість групової обробки файлів, щоб зберегти час і ресурси.

Автоматизація процесів: програмне забезпечення має дозволяти налаштовувати автоматичні сценарії обфускації або видалення метаданих під час створення, редагування або передачі файлів.

Інтеграція із зовнішніми системами: для зручності використання програмне забезпечення повинно підтримувати інтеграцію з іншими додатками та файловими системами, щоб автоматично обробляти файли, що зберігаються або передаються через ці системи.

2. Інтерфейс користувача

Інтерфейс програмного забезпечення повинен бути інтуїтивно зрозумілим, навіть для користувачів без технічного досвіду. Основні компоненти інтерфейсу могли б включати:

Головна панель: користувачі бачать список завантажених файлів із метаданими, які можна переглядати, редагувати або видаляти.

Інструменти для обфускації: кнопки або меню для вибору різних методів обфускації (шифрування, маскування, фальсифікація) з можливістю застосування їх до конкретних метаданих.

Налаштування автоматизації: розділ для налаштування автоматичних правил обробки файлів, наприклад, автоматичне видалення або обфускація метаданих під час завантаження файлу.

Панель інструментів для групової обробки: можливість завантажувати й обробляти кілька файлів одночасно з налаштуванням однакових правил для всіх вибраних файлів.

Історія обробки: розділ, де відображаються дії, виконані з файлами, що дозволяє відслідковувати, коли і які метадані були обфусковані або видалені.

Таке програмне забезпечення може знайти застосування у компанії, яка регулярно публікує звіти, презентації та документи для зовнішніх партнерів. Перед публікацією файлів система автоматично сканує їх на наявність метаданих, таких як імена співробітників, геолокація або дати редагування. Якщо виявляються чутливі дані, система автоматично обфускує їх, зберігаючи функціональність документів для перегляду та редагування, але приховуючи конфіденційні метадані.

Для подальшої автоматизації процесу захисту метаданих передбачається застосування таких технологій, як машинне навчання для аналізу та класифікації метаданих перед обфускацією, а також хмарні сервіси для синхронізації даних між різними пристроями користувачів. У системі також планується інтеграція з API для захисту метаданих у реальному часі під час передачі файлів через мережі.

Захист метаданих за допомогою обфускації та інших методів — це важливий елемент інформаційної безпеки. Використання спеціалізованого програмного забезпечення, яке автоматизує ці процеси, значно спрощує захист даних і мінімізує ризики витоку інформації через метадані.

Висновки. У процесі розгляду теми захисту метаданих за допомогою обфускації було досліджено природу метаданих, їхню важливість та потенційні загрози, які можуть виникати внаслідок їхньої незахищеності. Метадані є не лише невід'ємною частиною сучасних інформаційних систем, але й становлять значну загрозу для конфіденційності, оскільки можуть розкрити важливу інформацію про файли, їх авторів, місце створення та інші деталі. У цьому контексті обфускація метаданих виступає як ефективний засіб захисту. Вона дозволяє приховувати або спотворювати інформацію таким чином, щоб зловмисники не могли легко її зрозуміти або використовувати. Серед основних методів обфускації варто виділити шифрування, маскування даних, фальсифікацію та видалення метаданих, кожен із яких має свої переваги та обмеження.

Застосування обфускації стає особливо актуальним у світлі сучасних кіберзагроз та постійно зростаючого обсягу даних, що обробляються в цифрових системах. Окрім того, для ефективного захисту метаданих важливо використовувати комплексний підхід, що включає не лише обфускацію, але й інші методи захисту, такі як шифрування та управління доступом. У практичному розділі ми розглянули можливі підходи до автоматизації процесу захисту метаданих, зокрема через розробку спеціалізованого програмного забезпечення. Запропоноване програмне забезпечення може автоматично аналізувати, обфускувати та видаляти метадані, забезпечуючи захист конфіденційної інформації під час роботи з великими обсягами файлів.

Таким чином, впровадження обфускації як методу захисту метаданих є важливим кроком у забезпеченні інформаційної безпеки в сучасних умовах. Надійне програмне забезпечення для автоматизації цього процесу може стати ключовим інструментом для компаній та організацій, що прагнуть захистити свої дані від несанкціонованого доступу та використання.

Список літератури

1. Smith J., Brown, L. The Risks of Metadata Exposure in Digital Communication. *Cybersecurity Journal*. 2022. V.14(3). P. 112-126. URL: https://cybersecjournal.com/metadata_risks
2. Johnson A. Metadata in Cloud Storage: Vulnerabilities and Protection Strategies. *International Conference on Information Security*. 2020. DOI:10.1007/978-3-030-12345-1
3. ExifTool: A comprehensive tool for metadata editing. Available: https://exiftool.org
4. Metadata Anonymization Toolkit (MAT). URL: https://mat.boum.org
5. Case Study: How a London company lost $500,000 due to metadata breaches. URL: https://www.cybersecurityexamples.com/case-london
6. Blender Plugin for Metadata Protection. Blender Community. URL: https://community.blender.org/plugins/metadata_protection
7. Palmer R. Encryption and Masking of Metadata: A Guide for Corporate Security. *Information Security Quarterly*. 2021. V.22(2). P. 78-90. DOI: 10.1016/j.infsec.2021.03.002
8. Harris T., Mitchell, P. 3D Model Intellectual Property Protection Using Digital Watermarks. *Journal of Digital Media Securit.* 2019. V.15(1). P. 45-59. URL: https://doi.org/10.1007/s00329-019-01451
9. Yang Z., Lee D. Techniques for Automated Metadata Obfuscation in Large-Scale Systems. *Security and Privacy in Computing*.2021. DOI: 10.1109/SPC.2021.00132

Є.С. Булгаков, Н.І. Кушніренко, В.В. Подуфалов, В.О. Назаров

APPLICATION OF OBFUSCATION FOR PROTECTING FILE METADATA FROM UNAUTHORIZED ACCESS

E.S. Bulgakov, N.I. Kushnirenko, V.V. Podufalov, V.O. Nazarov

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
Email: infsec2011@gmail.com

This article addresses the issue of protecting file metadata from unauthorized access through obfuscation. Metadata plays a key role in modern digital systems, providing essential information about files, such as authorship, creation date, geolocation, device type, and other attributes that help identify and classify them. However, this data can become vulnerable to cyberattacks, as malicious actors may use metadata to gather confidential information or launch attacks on users and organizations. The article provides a detailed analysis of various metadata obfuscation methods, including encryption, masking, and falsification, each with its own advantages and disadvantages. Encryption ensures a high level of protection but requires key management, which can be challenging for large organizations. Masking involves replacing real metadata values with pseudonyms or random values, while maintaining file functionality. Metadata falsification involves creating false information to mislead attackers. In addition, the article proposes the concept of specialized software for automated metadata protection that allows users to automatically obfuscate or delete file metadata during processing or transmission over the network. The software also includes the ability to process files in bulk, which is crucial for organizations working with large amounts of data. Such solutions are highly relevant in the face of modern cyber threats, as they provide a high level of confidentiality and data protection. An important aspect is that the proposed software not only obfuscates data but also integrates with other systems to automate protection processes. Thus, the work highlights the importance of obfuscation as a tool for improving the level of information security and protecting confidential information. The proposed software solution represents a promising step toward addressing the issue of data leaks through metadata and can be applied in various industries, including medicine, education, architecture, and game development, where data protection is crucial.
Keywords: metadata protection, obfuscation, encryption, masking, falsification, software.