УДК 004.056

М.О. Притула
С. С. Штефанеса

АНАЛІЗ МЕТОДІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В РАДІОТЕХНІЧНИХ СИСТЕМАХ

Вінницький національний технічний університет

Анотація

У даній роботі розглянуто та досліджено методи криптографічного захисту інформації, поняття криптографії, криптології, типи шифрування та маскування даних, а також їх алгоритми. Розглянуто дані, які потребують маскування та шифрування. Проаналізовано фактори надійності методів криптографічного захисту інформації, їх переваги та недоліки.

Ключові слова: криптологія, криптографія, шифрування, маскування, криптостійкість.

Abstract

This paper examines and researches the subject of cryptographic information protection methods, the concepts of cryptography, cryptology, types of data encryption and masking, as well as their algorithms. Data that needs masking and encryption is considered. Reliability factors of cryptographic information protection methods, their advantages and disadvantages are analyzed.

Keywords: cryptology, cryptography, encryption, masking, crypto-resistance.

Вступ

В даний час в умовах швидкого розвитку інформаційних технологій та вдосконалення технічних засобів обробки, передачі та зберігання інформації, зростає не тільки кількість нових завдань у цій області, але і кількість технічних рішень вже відомих, традиційних завдань. Для цього ведеться пошук і створення нових технічних засобів. Актуальним завданням була і продовжує залишатися, зокрема, задача забезпечення конфіденційності при передачі та обробці інформації радіотехнічними системами. Із збільшенням кількості інформації та її ролі в інноваційному світі, актуальніше стає завдання захисту інформації від несанкціонованого доступу до неї. На новому етапі розвитку технологій, доступ до будь-якої інформації, яка передається каналами зв'язку, досить легко може бути реалізований за допомогою спеціальних технічних засобів. На жаль, на даний момент на всьому "ланцюжку" процесів генерації, шифрування і доставки інформації до споживача є багато "вузьких" місць, що сприяють витоку інформації. Одним з таких прикладів може бути витік інформації з вузлів електричних каналів зв'язку у вигляді електромагнітного поля, яке змінюється відповідно до сигналів переданої інформації. [1]

Як відомо, всі розглянуті методи захисту інформації, що містяться в сигналах, умовно можна розділити на дві категорії: перша шифрування і друга маскування. Отже, проведемо аналіз методів захисту інформації в радіотехнічних системах.

Результати дослідження

Криптографія вирішує проблеми пов'язані із захистом інформації шляхом їх перетворення. Вона займається проблемами аутентифікації, цілісності, конфіденційності та рядом інших пов'язаних завдань. Практична криптографія вивчає методи шифрування інформації, сертифікатами та управління ключами, створення електронного підпису. Криптоаналіз розглядає протилежні криптографічні завдання, зокрема, несанкціоноване дешифрування даних (без знання ключа). Криптологія - розділ математики, який вивчає математичні основи методів криптографії та криптоаналізу.

З усіх методів захисту інформації в радіотехнічних системах, шифрування є найпоширенішим. Це пов'язано з тим, що він підходить для будь-яких цілей. При використанні цього методу на сучасних гаджетах не потрібно використовувати всю потужність пристрою. Тому більшість месенджерів, встановлених на смартфонах і планшетах, шифрують усі повідомлення користувачів.

Шифрування – це метод маскування даних, який використовується для захисту від кіберзлочинців. Даними може бути вміст бази даних, повідомлення електронної пошти, миттєве повідомлення або файл, що зберігається на комп'ютері.

Існує багато методів шифрування текстових повідомлень і аудіофайлів. Однак не всі вони використовуються через різного ступеня надійності [1, 2].

Кожен метод шифрування оцінюється з точки зору таких факторів:

1. Криптостійкість. У програмуванні є такий термін як криптоатака. Це концепція, яка визначає процес дешифрування повідомлення шляхом вгадування ключів. Відповідно, криптографічна стійкість - це рівень надійності шифру, який визначається складністю підбору ключів. Найнадійніші методи - це ті, в яких для розшифрування повідомлення необхідно перерахувати всі можливі ключі.

2. Обсяг зашифрованого повідомлення. Оскільки для швидкої передачі інформації важливо зберегти її початковий обсяг, перевага віддається методам, у яких обсяг зашифрованого тексту дорівнює обсягу вихідного повідомлення або трохи перевищує його.

3. Наявність помилок. Деякі методи дають збій, через що вміст зашифрованих повідомлень частково або повністю втрачається. Тому в загальній практиці обраний метод шифрування перевіряється на наявність помилок перед впровадженням.

4. Швидкість шифрування та дешифрування. Чим швидше повідомлення шифрується, передається та розшифровується, тим вища популярність техніки, яка використовує даний метод. Сучасні методи дозволяють трансформувати інформацію за кілька секунд.

5. Цінова доступність використовуваних алгоритмів. Для оцінки їх ефективності вартість порівнюється з цінністю інформації та фінансовими наслідками від її витоку.

Виходячи з перелічених факторів, можна зробити висновок, що найбільш популярними та ефективними методами шифрування є надійні, швидкі, недорогі алгоритми, які не призводять до втрати даних або збільшення їх обсягу. Однак головну роль у цьому випадку відіграє криптографічна стійкість шифру, який використовується в радіотехнічній системі.

Криптостійкість забезпечується використанням секретного алгоритму шифрування та складних ключів. Однак не завжди вдається зберегти це в секреті. Тому розробники засобів криптографічного захисту інформації радіотехнічних систем намагаються створити надійні алгоритми з максимально можливою довжиною ключа [2, 3].

Методи шифрування можна класифікувати відповідно до типу ключа шифрування, який вони використовують для кодування та декодування даних:

1. Асиметричне шифрування. Цей метод також називають криптографією з відкритим ключем. Він шифрує та розшифровує інформацію за допомогою двох різних криптографічних асиметричних ключів (приватного ключа та відкритого ключа).

2. Симетричне шифрування. Цей метод використовує один закритий ключ для дешифрування та шифрування. Симетричне шифрування працює швидше, ніж асиметричне шифрування. Він найбільше підходить для використання окремими особами або в закритій системі. Використання симетричних методологій з декількома користувачами у відкритій системі, наприклад, через мережу, вимагає передачі ключа, що створює можливість крадіжки. Найпоширенішою формою симетричного шифрування є AES.

Розглянемо алгоритми шифрування.

Сьогодні стандарт шифрування даних DES є застарілим симетричним алгоритмом шифрування. В DES використовується один 56-бітний ключ шифрування та дешифрування даних в одиницях по 64 біти. Такі розміри, як правило, недостатньо великі для сучасних цілей. Таким чином, різні алгоритми шифрування витіснили DES.

Як і DES, Blowfish зараз застарів, проте цей застарілий алгоритм все ще дієвий. Цей симетричний шифр організовує повідомлення в блоки по 64 біти та шифрує їх по одному. Twofish замінив Blowfish.

Twofish використовується як в апаратних, так і в програмних складових радіотехничних систем. Twofish використовує ключі довжиною до 256 біт. Однак він залишається одним із найшвидших алгоритмів шифрування. Цей симетричний шифр не запатентований і безкоштовний.

Потрійний DES (3DES або TDES) запускає алгоритм DES тричі. Він шифрує, розшифровує та повторно шифрує для отримання довшого ключа. Його можна запускати лише за допомогою одного ключа, двох ключів або трьох окремих ключів — чим більше ключів, тим надійніша безпека. 3DES використовує методологію блокового шифрування, що робить його вразливим до атак, включаючи зіткнення блоків.

Розширений стандарт шифрування (AES) - симетричний алгоритм шифрування. Він шифрує блоки даних (128 біт) за один раз. Є три варіанти ключів, які використовуються для розшифровки тексту: 128-бітний ключ — шифрує інформацію за 10 циклів, 192-бітний ключ — шифрує за 12 циклів, 256-бітний ключ — шифрує за 14 циклів. Кожен раунд включає кілька кроків заміни,

змішування відкритого тексту, транспонування тощо. Стандарти шифрування AES є найпоширенішими сьогодні методами шифрування для даних при передачі та при зберіганні в радіотехнічних системах.

RSA - це асиметричний алгоритм шифрування. Він заснований на факторизації результату двох великих простих чисел. Тільки людина, яка знає ці номери, знатиме, як розшифрувати повідомлення. RSA зазвичай використовується під час передачі даних між двома окремими кінцевими точками. Однак він працює повільно під час шифрування великих обсягів даних.

ECC (шифри на еліптичних кривих) є швидкою та потужною формою шифрування даних, яка використовується як компонент протоколу SSL/TLS. Він використовує зовсім інший математичний процес, який дозволяє використовувати меншу довжину ключа для збільшення швидкості, водночас пропонуючи надійний захист. Наприклад, 3072-бітний ключ RSA та 256-бітний ключ ECC пропонують однакові рівні безпеки. [3]

Існують загальні критерії, які представляють собою перелік правил для перевірки стійкості заяв про безпеку продукту під час тестування. Шифрування спочатку не охоплювалося загальними критеріями, хоча зараз воно частіше входить до стандартів безпеки, викладених для проекту. Керівні правила загальних критеріїв були створені, щоб запропонувати сторонню, нейтральну до постачальників перевірку продуктів безпеки. Продавці добровільно представляють продукти для оцінки, а їх функціональні можливості вивчаються окремо або в цілому. Після оцінки продукту, його можливості та характеристики перевіряються відповідно до семи рівнів. Він також порівнюється з набором стандартів на основі типу продукту. [4]

Маскування даних - це техніка, яка використовується для створення версії даних, структурно подібної до оригіналу, але приховує (маскує) конфіденційну інформацію. Версію із замаскованою інформацією можна використовувати для різних цілей, наприклад для навчання користувачів або тестування продукту. Основною метою маскування даних є створення функціональної заміни, яка не розкриває справжні дані.

Існує широкий спектр способів, які можна використовувати для зміни даних, включаючи перетасування символів, заміну слів або символів і шифрування. Кожен метод має свої унікальні переваги. Однак під час маскування даних, значення завжди потрібно змінювати таким чином, щоб унеможливити зворотне перетворення [3,4].

Ось кілька прикладів маскування даних: заміна персональних даних та імен іншими символами та символами; переміщення деталей або рандомізація конфіденційних даних, таких як імена чи номери рахунків; шифрування даних, заміна їх частин іншими частинами з того самого набору даних; видалення або “обнулення” конфіденційних значень у записах даних; шифрування даних, щоб зробити неавторизованим користувачам доступ до них без ключа дешифрування.

Найпоширеніші типи даних, які потребують маскування даних:

1. Особиста інформація - дані, які можна використовувати для ідентифікації певних осіб. Це включає таку інформацію, як повне ім’я, номер паспорта, номер водійського посвідчення та номер соціального страхування.

2. Захищена медична інформація - дані, зібрані постачальниками медичних послуг з метою визначення належного догляду. Це включає інформацію про страхування, демографічну інформацію, результати аналізів і лабораторних досліджень, історії хвороби та стан здоров’я.

3. Інформація про платіжні картки. Стандарт безпеки даних платіжних карток (PCI DSS) вимагає від продавців, які обробляють транзакції за кредитними та дебетовими картками, належним чином захищати дані власників карток.

4. Інтелектуальна власність - дані, пов’язані з творіннями розуму, включаючи винаходи, бізнес-плани, проекти та специфікації, мають високу цінність для організації та мають бути захищені від несанкціонованого доступу та крадіжки.

Існують три типи маскування даних:

Статичне маскування даних - передбачає створення дубльованої версії набору даних, що містить повністю або частково замасковані дані. Фіктивна база даних зберігається окремо від основної бази даних.

Динамічне маскування даних - змінює інформацію в режимі реального часу, коли до неї звертаються користувачі. Ця техніка застосовується безпосередньо до основних наборів даних. Це гарантує, що вихідні дані бачать лише авторизовані користувачі, а будь-який непривілейований користувач бачить замасковані дані.

Маскування даних в процесі - змінює конфіденційну інформацію під час її передачі між середовищами, гарантуючи, що конфіденційна інформація маскується до того, як вона досягне

цільового середовища. Цей метод ідеально підходить для радіотехнінчих систем, які переносять дані між системами або підтримують безперервну інтеграцію чи синхронізацію різних наборів даних.

Розглянемо найпоширеніші методи маскування даних, які можна використовувати для захисту даних в радіотехнічних системах.

1. Псевдонімізація даних - дозволяє замінити вихідний набір даних на псевдонім. Цей процес є зворотним - він деідентифікує дані, але все ще дозволяє пізніше використовувати повторну ідентифікацію, якщо це необхідно.

2. Анонімізація даних - метод, який дозволяє кодувати ідентифікатори, які пов'язують осіб із замаскованими даними. Мета полягає в тому, щоб захистити приватну діяльність користувачів, зберігаючи достовірність замаскованих даних.

3. Пошукова підстановка. Ви можете замаскувати робочу базу даних за допомогою доданої таблиці пошуку, яка надає альтернативні значення оригінальним конфіденційним даним. Це дозволяє використовувати реалістичні дані в тестовому середовищі, не відкриваючи оригінал.

4. Шифрування. Таблиці пошуку легко зламати, тому рекомендується шифрувати дані, щоб отримати до них доступ лише за допомогою паролю. Дані не читаються під час шифрування, але доступні для перегляду після розшифрування, тому вам слід поєднати це з іншими методами маскування даних.

5. Редакція. Якщо конфіденційні дані не потрібні для забезпечення якості чи розробки, ви можете замінити їх загальними значеннями в середовищі розробки та тестування. У цьому випадку немає реалістичних даних із подібними атрибутами до оригіналу.

6. Усереднення

Якщо ви хочете відобразити конфіденційні дані в термінах середніх або сукупних значень, але не на індивідуальній основі, ви можете замінити всі значення в таблиці середнім значенням. Наприклад, якщо в таблиці наведено зарплати працівників, ви можете замаскувати фактичні індивідуальні зарплати, замінивши їх усі середньою зарплатою, щоб загальний стовпець відповідав справжньому загальному значенню сумарних зарплат.

7. Перетасування. Якщо вам потрібно зберегти унікальність під час маскування значень, ви можете захистити дані шляхом їх шифрування, щоб реальні значення залишалися, але призначалися іншим елементам.

8. Перемикання дат. Якщо спірні дані включають дати, які ви хочете зберегти конфіденційними, ви можете застосувати правила до кожного поля даних, щоб приховати справжню дату. Наприклад, можна відстрочити дати всіх активних контрактів на 100 днів. Недоліком цього методу є те, що, оскільки однакова політика застосовується до всіх значень у полі, компроміс одного значення призводить до компромісу всіх значень [4].

Основними проблемами пов'язаними з маскуванням даних є [5]:

1. Збереження формату - рішення для маскування даних має розуміти дані (тобто, що вони представляють). Коли система маскування замінює оригінальні дані неавтентичними даними, вона повинна зберігати вихідний формат. Це особливо важливо для потоків даних, які вимагають певного порядку або формату, наприклад дати.

2. Цілісність - таблиці в реляційній базі даних з'єднані через первинні ключі. Коли рішення маскування модифікує або замінює значення первинного ключа таблиці, ці значення необхідно змінювати послідовно в базі даних.

3. Семантична цілісність - бази даних зазвичай застосовують правила, які обмежують діапазон дозволених значень (наприклад, діапазон вхідних та вихідних рівнів сигналів). Будь-які замасковані дані мають входити до вказаного діапазону, щоб зберегти семантику (значення) даних.

4. Унікальність даних - під час маскування унікальних даних система маскування повинна застосовувати унікальні значення для кожного елемента даних. Наприклад, якщо у відповідній таблиці зберігаються перелік частот сигналів, кожна частота має отримати унікальний номер після маскування. Слід зберегти частотний розподіл замаскованих даних, особливо якщо розподіл є значущим (тобто географічний розподіл). Кожен стовпець у таблиці повинен мати в середньому подібні масковані значення даних до оригіналу [4].

Висновки

Отже, в даній роботі було проаналізовано методи та алгоритми криптографічного захисту інформації в радіотехнічних системах. Виявлено відмінність між маскуванням та шифруванням

даних, розглянуто відомі алгоритми шифрування даних та типи маскування даних, переваги та недоліки кожного з них.

В результаті чого можна зробити висновок що кожен із методів має своє призначення, шифрування - це метод маскування даних, який використовується для захисту від кіберзлочинців. Маскування - це техніка, яка використовується для створення версії даних, структурно подібної до оригіналу, але приховує конфіденційну інформацію. Основною метою маскування даних є створення функціональної заміни, яка не розкриває реальні дані. Із розглянутих алгоритмів шифрування даних розуміємо, що вибір конкретного алгоритму шифрування залежить від конкретних вимог та сценаріїв використання. Сучасні стандарти, такі як AES та ECC, часто є безпечними та ефективними варіантами для багатьох завдань шифрування даних серед всіх можливих. Також немає універсального методу маскування даних, який підходив би для всіх випадків. Вибір методу повинен враховувати специфіку даних, вимоги до безпеки та збереження приватності та цілісності, а також практичність застосування в конкретному контексті проекту. Зазвичай комбінація декількох методів може бути найкращим підходом для забезпечення максимального рівня захисту конфіденційних даних в радіотехнічних системах.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. 4 Cryptographic Techniques Used in Cybersecurity [Електронний ресурс] – Режим доступу до ресурсу: https://www.quickstart.com/information-security/4-cryptographic-techniques-used-in-cyber-security/.
2. Cryptographic methods of information security [Електронний ресурс] – Режим доступу до ресурсу: https://searchinform.com/challenges/information-security/information-security-basics/key-aspects-of-information-security/the-basic-principles-of-information-security/information-security-methods/cryptographic-methods-of-information-security/.
3. What is the difference between Encryption and Masking? [Електронний ресурс] – Режим доступу до ресурсу: https://www.encryptionconsulting.com/education-center/encryption-vs-masking/.
4. Data Masking [Електронний ресурс] – Режим доступу до ресурсу: https://satoricyber.com/data-masking/data-masking-8-techniques-and-how-to-implement-them-successfully/.
5. Data Encryption [Електронний ресурс] – Режим доступу до ресурсу: https://satoricyber.com/data-masking/data-encryption-top-7-algorithms-and-5-best-practices/.

Притула Максим Олександрович *– к.т.н., старший викладач кафедри інформаційних радіоелектронних технологій і систем, Вінницький національний технічний університет, м. Вінниця, e-mail: pritulamo@ukr.net*

Штефанеса Сергій Сергійович *— студент групи КІВТ – 23м, факультет інформаційних електронних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: serhiishtefanesa@gmai.com*

Prytula Maksym Oleksandrovych *- Ph.D., Senior Lecturer of the Department of Information Radio Electronic Technologies and Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: pritulamo@ukr.net*

Shtefanesa Serhii Serhiyovich — *student of KIVT group - 23m, Faculty of Information Electronic Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: serhiishtefanesa@gmail.com.*