DOI https://doi.org/10.30525/978-9934-26-277-7-146

MECHANISMS OF CRYPTOGRAPHIC PROTECTION DURING USER AUTENTICATION IN DATA TRANSMISSION SYSTEMS

МЕХАНІЗМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ПРИ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ В СИСТЕМАХ ПЕРЕДАЧІ ДАНИХ

Lukina K. V.
Instructor of the Department of Construction of Telecommunication Systems
Military Institute of Telecommunications and Informatization named after Heroes of Kruty
Kyiv, Ukraine

Лукіна К. В.
викладач кафедри побудови телекомунікаційних систем
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут
м. Київ, Україна

Широке використання інформаційних технологій, створення єдиного інформаційного простору, в рамках якого відбувається накопичення, обробка, зберігання та обмін інформацією, призвело до різкого зростання обсягу інформації (у тому числі конфіденційної), яка передається по відкритих каналах зв'язку. Тому, проблема інформаційної безпеки набуває ще більшої актуальності. Відомо, що застосування різних методів автентифікації (множинної автентифкації) та їх комбінацій підвищує стійкість системи автентифікації і є однією з ключових елементів інфраструктури захисту інформаційних систем від несанкціонованого доступу (далі – НСД).

Проблема автентифікації вирішується шляхом застосування різних систем чи комплексів захисту.

Основні положення захисту інформації від НСД:

− доступ до інформації має тільки той користувач, який має дозвіл, так званий законний користувач;

− кожен законний користувач повинен працювати тільки зі своєю інформацією і не мати доступ до інформації іншого законного користувача;

− кожен законний користувач може виконувати тільки ті операції, які йому дозволено виконувати.

Для забезпечення цих положень, необхідне розпізнавання «законного» користувача, тобто – процес авторизації, що складається

з трьох етапів: ідентифікація користувача, його автентифікація та безпосередньо сама авторизація.

Запропонована концепція безпеки визначає процес перевірки достовірності облікових даних користувача та унеможливлює використання системи несанкціонованими користувачами.

Методи автентифікації поділяють на три групи [1], в залежності від наявності у користувачей: предмета з унікальною інформацією (наприклад, USB-ключ); інформації, яка є невід'ємною його частиною: біометрична автентифікація (відбиток пальця, сканування сітківки ока); знань певної унікальної конфіденційної або секретної інформації (наприклад, пароль).

До першої групи належать методи автентифікації, які передбачають використання перепусток, магнітних карт, носимих пристроїв, що широко застосовуються для контроля доступу в приміщення, а також входять до складу программно-апаратних комплексів захисту від НСД до засобів обчислювальної техніки.

До другої групи входять методи автентифікації, що грунтуються на застосування обладнання для вимірювання та порівняння з еталоном заданих індивідуальних характеристик користувача: відбитки пальців, структура сітківки ока і т.д. Ці методи мають високу точність аутентифікації, тому що підробити біометричні параметри неможливо.

Останню, третю групу, складають методи автентифікації, при яких використовують паролі. За економічними причинами вони включаються як базові, класичні засоби захисту у велику кількість програмно-апаратних комплексів захисту інформації. Всі сучасні операційні системи і багато з додатків мають вбудовані механізми парольного захисту. При цьому для усунення наслідків НСД супротивника до інформації, що зберігається, може бути як пароль, так і його хеш-функція.

Тобто, користувач може підтвердити свою справжність, якщо надасть хоча б один ідентифікатор із будь-якої з трьох груп.

Нажаль, жодний з перерахованих заходів не забезпечує повного захисту, а лише ускладнює дії зловмисника. Кожен з методів має свої недоліки.

Якщо в процесі аутентифікації беруть участь тільки дві сторони, що встановлюють достовірність один одного, то це є безпосередньою автентифікацією. Якщо крім цих двох сторін, є ще інші, допоміжні, то таку автентифікацію називають автентифікацією з участю довірчої сторони. Третю сторону називають сервером автентифікації або арбітром.

Якщо в процесі автентифікаіцї використовується тільки один спосіб автентифікації, то вона називається одно факторною автентифікацією, якщо – декілька – багатофакторною.

Але, для ідентифікації засобами криптографії всі ці три групи методів автентифікації можуть бути зведені до однієї – до автентифікації на основі володіння якої-небудь інформацією. Тобто, будь-які біометричні дані або інформація, що міститься на фізичному носії, може бути перетворена в унікальний ключ (при ідентифікації за допомогою криптографічної системи або протоколу) або пароль (при автентифкації або ідентифікації парольними схемами), який буде однозначно визначати користувача (суб'єкта).

При виконанні криптографічного протоколу автентифікації одна сторона пересвідчується в тому, що інша сторона, задіяна в процесі автентифікації, є ідентичною та в тому, що друга сторона є активною під час або безпосередньо перед моментом придбання доказів.

Криптографічний алгоритм, названий алгоритмом шифрування, є певною математичною функцією, яка використовується для шифрування і розшифрування. Точніше таких функцій дві: одна застосовується для шифрування, а інша – для розшифрування. Розрізняють шифрування двох типів: симетричне (із секретним ключем) та несиметричне (з відкритим ключем).

Наприклад, система WINDOWS NT – це приклад однобічної автентифікації. Для WINDOWS 2000 процедура входу в систему це протокол KERBEROS і випадок двобічної автентифікації [2].

Протоколи автентифікації характеризуються: обчислювальною характеристикою, комунікаційною ефективністю, наявністю третьої сторони, основою гарантій безпеки, способом зберігання критичної ключової інформації.

Ефективний захист від НСД можливий тільки при поєднанні різних методів: організаційних, технічних, нормативно-правових. Побудова систем ідентифікації та автентифікації дозволить перекривати канали НСД до інформації, шляхом обмеження доступу до інформації, яка захищається.

Найбільший інтерес при формуванні ключів виклікає перспективний напрямок використання фізичних признаків функціонування інформаційних систем для генерації випадкових послідовностей. Такі послідовності, як правило, містять в собі риси притаманні лише конкретному комплекту телекомунікаційного обладнання. Згенерована послідовність цілком контрольована та не

можлива в підробці, оскільки фізичні процеси старіння, які відбуваються в устаткуванні, сутоіндівідуальні та не статичні [3].

На сьогодні криптографічні методи захисту інформації від несанкціонованого доступу є основним засобм захисту при передачі інформації по каналам зв'язку. Доцільно використовувати криптографічний захист при зберіганні інформації, що дозволить, разом з мірами по обмеженню доступу, запобігти несанкціонованому доступу до інформації.

Література:

1. Десятов С. В. Сравнительный анализ достоинств и недостатков наиболее распространенных методов идентификации и аутентификации пользователей и других участников идентификационных процессов. URL: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-dostoinstv-i-nedostatkov-naibolee-rasprostranennyh-metodov-identifikatsii-i-autentifikatsii-polzovateley-i/viewer (дата звернення 21.11.2022).

2. Ахрамович. В. М. Ідентифікація й аутентифікація, керування доступом. Сучасний захист інформації. К. : ДУТ, 2016. No 4. С. 47–51.

3. V Kuzavkov Evalution of probabilistic characteristics of random signal source. *Сучасна спеціальна техніка.* 2021. 65(2). С. 19–28.