УДК 004.056

ПОБУДОВА ПІДСИСТЕМИ ЗАХИСТУ ПОШТОВИХ ПОВІДОМЛЕНЬ

О.Д. ТЕРЕЩЕНКО, М.В. ЗАХАРОВА, В.В ХАРЛАМОВА, М.В. ЛЮТА

Київський національний університет технологій та дизайну

Розглянуто проблеми безпеки поштових повідомлень, та методи їх вирішення за допомогою стійких криптографічних алгоритмів та механізмів цифрового підпису. Побудовано підсистему захисту поштових повідомлень, що складається з чотирьох рівнів: авторизація користувачів, розмежування прав доступу до ресурсів, захист повідомлень, контроль цілісності повідомлень.

Інтенсивність використання електронної пошти та широкий спектр атак на повідомлення створюють багато проблем захисту поштових повідомлень при передачі. Передане повідомлення на шляху прямування до поштового сервера адресата проходить безліч вузлів, на кожному з яких воно може бути перенаправлено, змінено або сфальсифіковано ім'я відправника. Тому для забезпечення захисту поштових повідомлень необхідно застосувати методи криптографічного захисту та механізми цифрового підпису, що повинні використовуватися на робочій станції відправника, до передачі повідомлення по мережі.

Постановка завдання

Метою роботи є побудова підсистеми захисту поштових повідомлень, що дозволить запобігти модифікації та перегляду повідомлення зловмисником на шляху слідування до адресата. Використання в підсистемі сучасних алгоритмів шифрування та механізмів цифрового підпису дозволить підвищити захищеність поштових повідомлень та вирішити проблему відмови від авторства.

Результати та їх обговорення

Для вирішення проблеми забезпечення захисту поштових повідомлень на заданому рівні, досягнення якого не вимагало б надмірних витрат, необхідний систематичний і комплексний підхід. Більшість проблем, пов'язаних безпосередньо з забезпеченням конфіденційності поштових повідомлень, закладалися при виникненні електронної пошти три десятиліття тому та залишаються не вирішеними і в наш час:

- ні один з стандартних поштових протоколів (SMTP, POP3, IMAP4) не включає механізмів захисту, які гарантували б конфіденційність листування;
- відсутність надійного захисту протоколів дозволяє створювати повідомлення з фальшивими адресами;
- електронні повідомлення легко модифікувати;
- відсутність перевірки цілісності повідомлення.

У відомих публікаціях щодо сучасних методів захисту інформації досить повно обґрунтовані об‘єктивні часткові задачі із гарантованого забезпечення надійного захисту та представлені раціональні шляхи їх вирішення, розглядаються основні принципи побудови систем захисту інформації, але відсутня

єдина концепція захисту поштових повідомлень при передачі. Тому необхідно розробити підсистему захисту, повинна будуватися як ієрархічна система - можуть бути виділені декілька основних рівнів ієрархії захисту. Виділення цих рівнів та їх реалізація є необхідною умовою побудови підсистеми захисту поштових повідомлень (Рис. 1).

Для ефективного забезпечення захисту повідомлень підсистема повинна містити наступні рівні:

- рівень авторизації користувачів;
- рівень розмежування прав доступу до ресурсів;
- рівень захисту повідомлень;
- рівень контролю цілісності повідомлень.

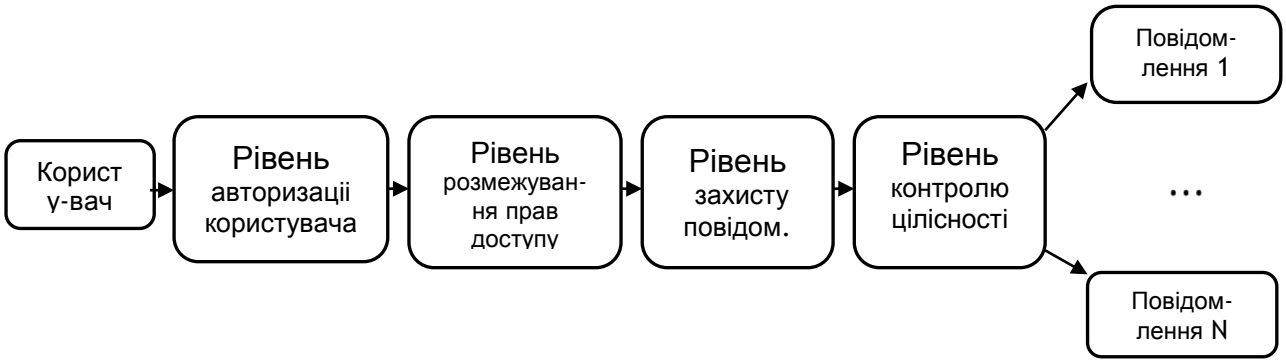

Рис. 1 **Схематичне відображення рівнів підсистеми захисту поштових повідомлень**

Рівень авторизації користувача служить для обмеження доступу до системи захисту. Цей рівень можна назвати базовим внаслідок того, що всі наступні рівні будуть працювати на основі результатів роботи рівня авторизації. У результаті чого, сам рівень авторизації повинен бути максимально захищений і добре продуманий.

Рівень управління доступом (розмежування прав доступу) на основі роботи рівня авторизації користувачів, реалізує власне розмежувальну схему доступу користувачів до ресурсів, що захищаються, а також політику адміністрування підсистеми захисту в рамках виконання політики інформаційної безпеки. Під підсистемою захисту тут розуміємо відповідні механізми, інших рівнів, бази даних, і конфігураційні файли підсистеми захисту.

Для вирішення завдання управління доступом до ресурсів, на цьому рівні їх можна розділити на ресурси: адміністратора та користувача.

До ресурсів адміністратора системи безпеки відноситься:

- генерація паролів;
- налаштування системи;
- адміністрування баз даних ключів;

До ресурсів користувача належить:

– прийом передача повідомлень;

– шифрування, дешифрування;

– цифровий підпис.

На цьому рівні також вирішується завдання розподілу функцій адміністрування безпекою підсистеми між користувачами:

– системним (мережевим) адміністратором;

– адміністраторами СУБД і додатків;

– адміністратором безпеки.

При цьому вирішується завдання централізації схеми адміністрування безпеки, в рамках якої, зміна параметрів безпеки на різних рівнях ієрархії підсистеми, повинна здійснюватися тільки при безпосередньому контролі з боку адміністратора безпеки.

Рівень захисту повідомлень перешкоджає несанкціонованій зміні та копіюванню до архіву повідомлень за допомогою стійких криптографічних алгоритмів, що розділені на класи:

– симетричні;

– асиметричні.

Симетричні системи шифрування діляться на два класи: блокові і потокові системи. Основний критерій такого поділу - потужність алфавіту, над знаками якого проводиться шифрування. Поділ шифрів на потокові та блочні пов'язаний з алгоритмічними і технічними особливостями реалізації шифруючих перетворень, що використовують можливості існуючої елементної бази (розрядність процесорів, швидкодію мікросхем, об'єм пам'яті комп'ютера). При збільшенні потужності алфавіту необхідно дослідити, перш за все, питання про вибір перетворень, реалізованих кріптосхемою, і способі їх практичної реалізації, що впливає на ефективність функціонування кріптосхеми з точки зору експлуатаційних характеристик

Асиметричні системи або системи шифрування з відкритим ключем можуть використовуватися для організації конфіденційного зв'язку в мережі користувачів.

Кожен з кореспондентів системи має ключ

$$k = (k_z, k_p), \tag{1}$$

що складається з відкритого ключа k_z і секретного ключа k_p. Відкритий ключ визначає правило шифрування E_k, а секретний ключ - правило дешифрування D_k. Ці правила пов'язані співвідношенням

$$D_k(E_k(M)) = C \tag{2}$$

для будь-якого відкритого тексту повідомлення M і будь-якого шифрованого тексту повідомлення C.

Знання відкритого ключа не дозволяє за прийнятний час (або з прийнятною складністю) визначити секретний ключ.

Раціонально використовувати блочні алгоритми, так як вони достатньо надійні і швидкі в роботі, наприклад, алгоритмів RC4, RC5, CAST, DES, AES [2]. Оптимальна довжина ключів шифрування для цих алгоритмів – 128 розрядів. Істотним недоліком алгоритмів даного типу є необхідність зберігання та передачі секретного ключа.

Асиметричні алгоритми, такі як RSA, Diffie-Hellman і El-Gamal при довжині ключа в 2048 розрядів володіють високою надійністю і не вимагають передачі секретного ключа. Але зведення в ступінь великих чисел займає досить багато часу [2].

Рішення проблеми вибору криптографічних алгоритмів шифрування електронних повідомлень може бути застосування блочного алгоритму для шифрування тексту повідомлення, і асиметричного - для шифрування ключа блокового алгоритму. Такий підхід дозволить швидко та надійно забезпечити захист переданого повідомлення з найменшими часовими витратами.

Рівень контролю цілісності призначений для вирішення проблем виявлення зміни тексту зашифрованого повідомлення під час проходження вузлів мережі від відправника до одержувача та фальсифікації імені відправника. Вирішити ці проблеми можливо використанням механізмів цифрового підпису, що дозволяє бути впевненим у відправнику повідомлення і його цілісності.

Цифровий підпис для повідомлення є числом, що залежать від самого повідомлення і від деякого секретного відомого тільки відправнику, ключа. При цьому передбачається, що підпис повинен легко перевірятися і що здійснити перевірку підпису повинен мати можливість кожен без отримання доступу до секретного ключа. При виникненні спірної ситуації, пов'язаної з відмовою підписувача від факту підпису їм деякого повідомлення або зі спробою підробки підпису, третя сторона повинна мати можливість вирішити суперечку.

Цифровий підпис дозволяє вирішити наступні задачі:

- здійснити аутентифікацію джерела повідомлення;
- встановити цілісність повідомлення;
- забезпечити неможливість відмови від підпису факту конкретного повідомлень.

Висновки

У даній роботі для вирішення проблем захисту поштових повідомлень, а саме: модифікації повідомлень під час передачі, фальсифікації імені відправника, відмови від авторства повідомлення, запропоновано підхід до побудови підсистеми захисту поштових повідомлень, що складається з чотирьох рівнів: авторизація користувачів, розмежування прав доступу, захист повідомлень, контроль цілісності повідомлення. Ієрархічне розташування в підсистемі всіх рівнів дозволяє ефективно захистити передане повідомлення від несанкціонованого доступу, визначати зміну зловмисником тексту повідомлення під час передачі. Побудована підсистема дозволяє підвищити захищеності поштових повідомлень при передачі від відправника до одержувача

ЛІТЕРАТУРА

1 Вильям Столлингс «Основы защиты сетей. Программы и стандарты». Вильямс. –2002 – 432 с.

2 Гнедов Г.Г. «Современные системы криптографической защиты информации».– К.: –2002 – 31 с.

3 Домарев В.В. «Безопасность информационных технологий. Методология построения систем защиты» «КМД ДС». –2001 – 688 с.

4 Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. «Защита информации в компьютерных сетях» – М.: –2001 – 375 с.