стану в стан під дією пуасоновських потоків випадкових подій. При цьому система *S* називається системою з дискретними станами, якщо вона має перераховану (або кінцеву) множину можливих станів $S_0, S_1, S_2, ..., S_k, ...$ і перехід з одного стану в інший здійснюється скачком.

Якщо такі переходи можливі в будь-який момент часу, то відбувається в системі *S* процес називається процесом з неперервним часом.

Для опису випадкового марківського процесу з дискретними станами $S_0, S_1, ...$ і безперервним часом користуються ймовірностями станів

$$p_0(t), p_1(t), p_2(t), ..., p_k(t), ..., \quad (5)$$

де $p_k(t)$ - ймовірність того, що система (процес) у момент *t* знаходиться в стані S_k.

При вивченні процесів, що протікають в системах, однією з основних завдань дослідження є визначення ймовірностей (5) по поставлених початкових умовах і умові нормування

$$\sum p_k(t) = 1.$$

Дані ймовірності, хоча і не описують процес вичерпним чином, все ж таки дають про нього досить повне представлення.

Висновок. Геометрично марківський процес зображується розміченим графом станів, відповідно до яких за певними правилами складається система лінійних диференціальних рівнянь ймовірностей станів $S_0, S_1, ...$[4]. Будь – якому графу однозначно відповідає система диференціальних рівнянь шуканих ймовірностей (5), і навпаки [4].

Фізичні системи, в яких відбуваються марківські процеси з неперервним часом, називають пуасонівськими системами. При цьому пуасонівська система є канонічною (або простої), якщо потоки, що визначають її стан, крім властивостей ординарності і відсутності післядії наділені властивістю стаціонарності, тобто, незмінністю у часі. Такою властивістю, як це випливає з (3), (4), мають лише ті потоки, в яких час між подіями розподілено за законом (2 ’).

Література

1. Галицкий А.В. Защита информации в сети – анализ технологий и синтез решений. / Галицкий А.В., Рябко С.Д., Шаньган В.Ф. – М.: ДМК Пресс, 2004. – 616 с.: ил.

2. Мясіщев О.А. Напрямки вирішення проблем захисту інформації в мережах. / Мясіщев О.А., Джулій А.В // Вісник Хмельницького національного університету – 2009. – № 4. – С. 107 – 111

3. Овчаров Л.А. Прикладные задачи теории массового обслуживания. / Овчаров Л.А. – М.: «Машиностроение», 1969. – 324с.

4. Эльсгольц Л. Э. Дифференциальные уравнения и вариационное исчисление. / Эльсгольц Л.Э. – М.: «Наука», 1969. – 424 с.

Надійшла 6.4.2011 р.

УДК 004: 004.65

В.М. ДЖУЛІЙ, О.Ю. ХМЕЛЬНИЦЬКИЙ
Хмельницький національний університет

АНАЛІЗ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ У КОМП’ЮТЕРНИХ СИСТЕМАХ

У статті проведено дослідження аналізу методів захисту інформації, що пересилається комп’ютерними системами та становить близько 75 % обсягу інформації, що пересилається через мережі. Часто в таких системах для забезпечення безвідмовності мережі та/або прискорення завантаження, дані зберігаються з надмірним використанням копії файлів або їхніх частин на різних комп’ютерах в мережі. Також можливий варіант, при якому файл ділиться на n частин так, що будь-яких K (K < n) з них досить, щоб відновити файл. Для забезпечення захисту та конфіденційності інформації в когмп’ютерних системах часто використаються криптосистеми з відкритим ключем. Зокрема, їх можна використати для побудови математичної моделі контролю доступу в комп’ютерній системі.

Research of analysis methods for protecting the information that peresylayet computer systems and is about 75 % of the amount of information sent over the network. Often in such systems to ensure the reliability of network and/or faster, the data stored with excessive use of copies of files or their parts on different computers on the network. Also possible in which the file is divided into five parts so that any K (K <n) are enough to restore the file. To ensure the security and confidentiality of information in computer systems are frequently used public key cryptosystem. In particular, they can be used to construct a mathematical model for access control in computer systems.

Ключові слова: система захисту інформації, комп’ютерні системи, конфіденційність інформації.

Вступ. Фахівці в області захисту інформації пропонують розділяти систему безпеки на дві частини: внутрішню і зовнішню [1]. У внутрішній частині здійснюється, в основному, контроль доступу шляхом ідентифікації і аутентифікації користувачів при допуску в мережу і при доступі в базу даних. Крім цього

шифруються і ідентифікуються дані під час їхньої передачі і зберігання. Безпека в зовнішній частині мережі в основному досягається криптографічними засобами.

За результатами проведених досліджень було визначено основні вразливі місця в мережевих системах [2]. Ними, як правило, є апаратура, інформаційний сервер, паролі і середовище передачі даних. Якщо інформаційний сервер може бути захищений організаційними заходами, то середовище передачі даних так не захистиш. Один із підходів захисту інформації за допомогою шифрування є використання спеціального програмного забезпечення. Стисло розглянемо деякі з них що з'явилися останнім часом.

Основні положення. На сучасному етапі технологічного розвитку суспільства та використання ним мереж та мережних технологій постає гостре питання безпеки передачі та зберігання інформації. Вагоме місце у програмному забезпечені для мережі та мережних технологій займають файлові системи. Як приклад можна привести Napster, Gnutella, Freenet, OceanStore, eDonkey, BitTorrent, а також системи на основі протоколу FastTrack: Kaza, Grokster, Morpheus та ін. [1]. За деякими відомостями [2], обсяг даних, що пересилають такими системами, становить близько 75 % обсягу інформації, що пересилається через мережу. Часто в таких системах для забезпечення безвідмовності мережі та/або прискорення завантаження, дані зберігаються з надмірним використанням копії файлів або їхніх частин на різних комп'ютерах в мережі. Також можливий варіант, при якому файл ділиться на п частин так, що будь-яких К (К < п) з них досить, щоб відновити файл. Для забезпечення конфіденційності інформації в розподілених системах часто використаються криптосистеми з відкритим ключем. Зокрема, їх можна використати для побудови математичної моделі контролю доступу в розподіленій системі [3].

Уперше криптосистема з відкритим ключем на лінійних кодах була запропонована Р. Мак-Элісом в 1978 році яка на сьогоднішній день так і залишається вагомим конкурентом серед інших систем [4]. При всіх перевагах використання таких систем виникають проблеми які пов'язані з певними факторами що безпосередньо впливають на роботу та стійкість криптосистем.

Такі фактори можна поділити на наступні групи:

1. Неможливість застосування стійких алгоритмів:
   - низька швидкість стійких криптоалгоритмів;
   - експортні обмеження;
   - використання власних криптоалгоритмів.
2. Невірна реалізація криптоалгоритмів:
   - зменшення криптостійкості при операції генерації ключа;
   - відсутність перевірки на слабкість створеного ключа;
   - недостатня захищеність від руйнуючих програмних засобів (віруси);
   - наявність залежності від часу опрацювання ключів;
   - помилки в програмній реалізації;
   - наявність запасних виходів;
   - недостатки в роботі датчика випадкових чисел.
3. Неправильне застосування криптоалгоритмів:
   - недостатня довжина ключа;
   - повторне накладання гами шифру;
   - зберігання ключа разом з даними.
4. Людський фактор.

До переваг подібних криптосистем можна віднести порівняно високу швидкість шифрування/розшифрування даних. Крім того, деякі із криптосистем на лінійних кодах можуть бути використані для одночасного шифрування й завадостійкого кодування даних, або ж для одночасного шифрування повідомлення й поділу його на частини – за схемою поділу секрету.

Розробка криптосистем для таких задач як захист, збереження цілісності та конфіденційності інформації в комп'ютерних системах передачі даних на сьогоднішній день є важливим питанням. Але у процесі створення таких алгоритмів виникає низка проблем, зокрема вони виражені у недоліках які мають власне самі децентралізовані системи обміну даними. Висока надійність таких систем призводить до дуже серйозних проблем пов'язаних з керуванням системою та достовірністю розповсюдженої в ній інформації та викликає ряд недоліків: керування системою; інформаційна відповідність; безпека; великі затрати на підтримку мережі; виникнення великої кількості помилок.

Важливим недоліком такої системи також є факт «паразитного підключення». Під цим терміном розуміють те що більшість користувачів не відкривають доступ до власних файлів а лише користуються відкритими. Таким чином перетворюючи систему з децентралізованою архітектурою на клієнт-серверну систему. На ряду з низкою проблем також можна визначити значні переваги: стрімке зростання кількості абонентів; стійкість системи відносно до збоїв; стійкість відносно зовнішніх технологічних втручань; масштабування системи; балансування навантаження; широкою смугою пропуску.

Такі переваги ставлять децентралізовані комп'ютерні системи на крок попереду перед іншими. Область застосування даних систем досить велика але найбільш успішними є лише чотири з них такі як:

- системи обміну файлами (file-sharing). У цьому випадку децентралізовані мережі виступають гарною альтернативою FTP-архівам, які вже давно перестали справлятися з ростом інформаційного наповнення та числа користувачів;

- розподілені обчислювальні мережі. Наприклад, такі як SETI@HOME. Цей проект продемонстрував величезний обчислювальний потенціал для добре не паралельних завдань. У даний момент у ньому беруть участь понад три мільйони користувачів, а загальне число «процесоро-років» перебільшило сімсот тисяч, і все це на абсолютно безкоштовній основі, коли добровольці не одержують крім можливості суспільного визнання;
- служби повідомлень (Instant-messaging);
- мережі групової роботи (P2P Groupware). Подібні додатки поки мало поширені, але в їхньому майбутньому сумніватися не доводиться. Одними із самих перспективних вважаються Groove Network – мережа, що надає захищений простір для комунікацій, і OpenCola – технологія пошуку інформації й обміну адресами найцікавіших джерел, де в ролі пошукового сервера виступає не персональний комп'ютер, а кожен з користувачів мережі, що обіцяє набагато більше високу дієздатність (при відповідальному підході користувачів до процесу).

Для вирішення проблеми безпеки передачі інформації в таких системах пропонуються наступні методи:

- побудова та аналіз математичної моделі децентралізованої системи;
- побудова та аналіз криптосистем з відкритим ключем;
- дослід принципів роботи децентралізованої системи;
- побудова та аналіз математичної моделі контролю доступу до файлів та директорій;
- побудова та аналіз математичної моделі контролю доступу до файлової системи.

Таким чином створення математичної моделі контролю доступу на основі криптосистеми з відкритим ключем на лінійних кодах з успіхом можуть застосовуватися для забезпечення захисту інформації від несанкціонованого доступу в децентралізованих файлових системах в умовах відсутності єдиного центру, що дозволяв або забороняв би доступ до файлів. Дана криптосистема з відкритим ключем може бути використана в системах передачі даних для забезпечення конфіденційності переданої інформації, особливо у випадку, коли необхідна висока швидкість шифрування та розшифрування даних що є важливим аспектом дослідження. Така система захисту на основі криптоалгоритмів дозволяє безпечно зберігати інформацію на довільному ПК від якого не вимагатиметься потужність опрацювання мережних операцій.

Висновки. По результатах проведених досліджень було визначено основні вразливі місця в мережевих системах. Ними, як правило, є апаратура, інформаційний сервер, паролі і середовище передачі даних. Якщо інформаційний сервер може бути захищений організаційними заходами, то середовище передачі даних так не захистиш. Відзначимо, що сучасна надійна криптографічна система повинна задовольняти наступним вимогам:

- процедури шифрування і дешифрування повинні бути "прозорі" для користувача;
- дешифрування закритої інформації повинно бути максимально ускладнене;
- зміст переданої інформації не повинен позначатися на ефективності криптографічного алгоритму;
- надійність криптозахисту не повинна залежати від утримання в секреті самого алгоритму шифрування (прикладами цього є як алгоритм DES, так і алгоритм ГОСТ 28147-89).

На сьогодні склалася думка, що створити криптографічний алгоритм легко, і такі алгоритми реалізуються багатьма незалежними програмістами і фірмами. Проте реально оцінити стійкість цих алгоритмів не можливо, оскільки більшість їх творців не бажає їх розкривати, посилаючись на комерційну таємницю, а це не дає можливості провести криптоаналіз таких алгоритмів. Не варто розраховувати на те, що стійкість цих алгоритмів вища, ніж у тих, які були опубліковані.

Література

1. Галицкий А. В., Рябко С. Д., Шаньган В. Ф. Защита информации в сети – анализ технологий и синтез решений. – М.: ДМК Пресс, 2004. – 616 с.: ил.

2. Норткатт С., Новак Д., Маклахлен Д. Обнаружение вторжений в сеть. Издательство "ЛОРИ", 2001, – 384 с.

3. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи // Москва: Мир. 1982.

4. T. ElGamal. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Trans. Inform. Theory. V. 31. P. 469-472. 1985.

Надійшла 27.4.2011 р.