Література

1. Широкополосные беспроводные сети передачи информации. Вишневський В.М., М: . Техносфера, 2005.
2. Цифровая связь. Б.Скляр. Москва, Санкт-Петербург, Киев, 2003.
3. http://www.softco.ru/80216.htm.

Надійшла до редакції
14.3.2011 р.

УДК 004: 004.65

О.Ю. ХМЕЛЬНИЦЬКИЙ
Хмельницький національний університет

УТОЧНЕННЯ ЗАГРОЗ ТА АНАЛІЗ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

В статті розглянуто принципи захисту інформації, що базуються на сучасних методах криптографії – які вирішують два головних питання: надійність і швидкодія. Розробка шифрів та програмного забезпечення, що відповідає цим умовам, знаходиться в центрі уваги дослідження. Головною причиною захисту інформації з використанням криптографії є здатність закриття конфіденційної інформації з певними гарантіями для її власника.

In the article the principles of information security, based on modern methods of cryptography – that solve two major issues: the reliability and performance. Development of codes and software that meets these conditions is the focus of research. The main prchynoyu protection using cryptography is the ability to close the confidential information with certain guarantees for its owner.

Ключові слова: криптографія, захист інформації.

Для більшості організацій захист мережевих ресурсів від несанкціонованого доступу на сьогодні стає однією з найгостріших проблем. Тривогу викликає той факт, що Internet в даний час використовується для транспортування і зберігання різних даних і конфіденційної корпоративної інформації. Такі побоювання є обгрунтованими, оскільки обмін даними переважно відбувається через відкриті базові мережі.

Існуючі методи захисту інформації базуються на сучасних методах криптографії – які повинні вирішити, в першу чергу, два головних питання: надійність і швидкодія. Розробка шифрів та програмного забезпечення, що відповідає цим умовам, знаходиться в центрі уваги багатьох досліджень [1]. Сильною стороною використання криптографії є здатність закриття конфіденційної інформації з певними гарантіями для її власника. Хоча цей напрям також має свої недоліки:

- труднощі розподілу зашифрованої інформації між декількома користувачами;
- накладні витрати від можливого зниження швидкості.

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.

По результатах 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.

Відома фірма RSA Data Security випустила нову версію популярного інструментального комплекту BSafe для мови програмування Internet-додатків Java. Новий продукт RSA, одержав назву Jsafe. За допомогою якого розробники зможуть вбудовувати в Java-додатки і аплети різні функції забезпечення безпеки, зокрема шифрування з відкритим і закритим ключем. JSafe функціонує на рівень нижче за Java-інтерфейс прикладного програмування Crypto API. Розробники можуть, таким чином, використовувати звичайний Crypto API, необхідно тільки вказати, що додаток повинен використовувати механізм криптозахисту JSafe. До складу JSafe входять алгоритми шифрування із закритим ключем RC2, RC4 і RC5, алгоритми формування сертифікатів цілісності повідомлень MD-5 і SHA-1, а також алгоритми хешування для формування цифрових підписів. Крім того, JSafe підтримує такі стандарти управління цифровими сертифікатами і обміну повідомленнями, як формат повідомлень PCKS#7 і алгоритм аналізу цифрових сертифікатів X.509.

Відомий інструментальний комплект JDK (Java Development Kit) версії 1.1 фірми JavaSoft надає лише обмежений набір таких засобів, включаючи шифрування на основі стандартних алгоритмів, проте він не підтримує методів шифрування з відкритим і закритим ключем. Саме ці методи складають основу сучасних засобів захищеної передачі даних по Internet, зокрема протоколу SSL (Secure Socket Level – захищений шар сокета).

Розглядаючи протоколи, що дозволяють згортати і приховувати від сторонніх очей протоколи високого рівня, шифруючи, а також підтверджуючи їх походження і цілісність, найбільше поширення набув SSL. Виробники програмного забезпечення стали вбудовувати SSL-функціональність в серверне і клієнтське забезпечення. Проте через обмеження експорту стійкого шифрування із США, на ринку в основному присутні "експортні" версії продуктів з бутафорською 40-бітовою криптографією. Тому найпопулярнішими захищеними серверами є безкоштовний Apache (в поставці SSL-Apache неамериканського походження) і комерційний Stronghold також неамериканський.

До засобів побудови комплексної системи інформаційної безпеки відносять також засоби аналізу захищеності. На сьогоднішній день відомо більше 60 засобів аналізу захищеності. Сказати який з них є кращим не можна. Кожен з цих засобів має свої переваги і недоліки. Одні призначені тільки для однієї операційної системи (як правило, UNIX), інші вимагають дуже глибоких знань архітектури мережі і ОС (SATAN), треті використовують для тестування тільки одну з уразливостей мережі (наприклад, Crack). Тому, перш ніж вибирати засіб аналізу захищеності, необхідно ретельно аналізувати особливості програмного і апаратного забезпечення, що використовується у мережі, і виходячи з цього, зробити вибір.

На Україні найбільш використовуваними в мережах є операційні системи UNIX і Windows NT. Причому часто дані ОС використовуються в рамках однієї мережі. Проте використанням всіх вище описаних засобів процес забезпечення безпеки не завершується. З часом наявні засоби захисту застарівають, виходять нові версії систем забезпечення інформаційної безпеки, постійно розширюється список знайдених уразливостей і атак. Тому фахівцям в області захисту інформації необхідна своєчасна і повна інформація про такі події.

Існуюча система криптографії використовує два типи криптографічних алгоритмів: класичні алгоритми, основані на використанні закритих, секретних ключів (симетричні) і алгоритми з відкритим ключем, в яких використовують один відкритий і один закритий ключ (асиметричні). Для класичної криптографії характерне використання однієї секретної одиниці – ключа, який дозволяє відправнику зашифрувати повідомлення, а одержувачу розшифрувати його. Секретні ключі є основою криптографічних перетворень, для яких, слідуючи правилу Керкхофа, стійкість хорошої шифрувальної системи визначається лише секретністю ключа [2].

У сучасних системах реалізовано досить багато різних алгоритмів криптографічного захисту інформації. Серед них можна назвати алгоритми DES, Rainbow (США); FEAL-4 і FEAL-8 (Японія); B-Crypt (Великобританія); алгоритм шифрування ГОСТ 28147-89 (Росія) і ряд інших, реалізованих постачальниками програмних і апаратних засобів захисту.

Відомий алгоритм, викладений в стандарті DES (Data Encryption Standard), прийнятий як федеральний стандарт в 1977 році, найбільш поширений і широко застосовується для шифрування даних в США. Лише деякі дані, методи захисту яких, визначаються спеціальними актами, не захищаються стандартом DES. Алгоритм DES достатньо надійний. Він володіє великою гнучкістю при реалізації різних додатків обробки даних, оскільки кожний блок даних шифрується незалежно від інших. Це дозволяє розшифровувати окремі блоки зашифрованих повідомлень або структури даних, а отже, відкриває можливість незалежної передачі блоків даних або довільного доступу до зашифрованих даних. Алгоритм може реалізовуватися як програмним, так і апаратним засобами. Істотний недолік даного алгоритму – мала довжина ключа.

Російський алгоритм шифрування, визначений стандартом ГОСТ 28147-89, є єдиним алгоритмом криптографічного захисту даних для великих інформаційних систем, локальних обчислювальних мереж і автономних комп'ютерів. Даний алгоритм може реалізовуватися як апаратним, так і програмним засобами, задовольняє всім криптографічним вимогам, що склалися в світовій практиці, і, як наслідок, дозволяє здійснювати криптографічний захист будь-якої інформації, незалежно від ступеня її секретності. Значним недоліком даного алгоритму – велика складність його програмної реалізації і низька швидкість роботи.

При аналізі алгоритмів шифрування, розроблених останнім часом, інтерес представляє алгоритм RC6 фірми RSA Data Security. Алгоритм RC6 є еволюційним удосконаленням відомого алгоритму RC5. Статистичні тести даного алгоритму показали добрі результати, що говорить про "якість" шифру. Працюючи одночасно з чотирма повними словами і використовуючи примітивні операції, які підтримуються більшістю процесорів, алгоритм показав хороші часові дані. Даний алгоритм шифрування можна рекомендувати для шифрування даних на магнітних носіях. Головною серйозною проблемою симетричних криптосистем є передача секретного ключа (для цієї мети використовуються закриті лінії, кур'єри і т.д.).

Асиметричні алгоритми шифрування, які також називаються системами з відкритим ключем, на сьогоднішній день є перспективними системами криптографічного захисту. Їх суть полягає в тому, що ключ, що використовується для шифрування, відмінний від ключа дешифрування. При цьому ключ шифрування не секретний і може бути відомий всім користувачам системи. Відомо декілька криптосистем з відкритим ключем, наприклад схема Т. Эль-Гамаля (T. El Gamal), в якій використовується ідея криптосистеми, запропонована У. Діффі (W. Diffie) і М. Е. Хеллманом (M. E. Hellman), криптосистема RSA і ін. Системи з відкритим ключем більше підходять для шифрування даних які передаються, ніж для захисту даних, які зберігаються на носіях інформації. Існує ще одна область використання асиметричних алгоритмів – цифрові підписи, які підтверджують достовірність переданих документів і повідомлень.

Асиметричні криптосистеми вважаються перспективними, оскільки в них не використовується передача ключів іншим користувачам і вони легко реалізуються як апаратним, так і програмним засобами. Проте системи типу RSA працюють значно повільніше, ніж класичні, і вимагають довжини ключа порядка 512 – 1024 біт. Тому всі їх переваги можуть бути зведені нанівець низькою швидкістю їх роботи. Крім того, для ряду функцій вже знайдені алгоритми інвертування, тобто доведено, що вони не є необоротними. Для функцій, що використовуються в системі RSA, такі алгоритми не знайдені, але немає і доказу безповоротності використовуваних функцій.

Висновки

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.

Надійшла до редакції
22.2.2011 р.

УДК 004.89

Т.О. САВЧУК, О.В. СМИРНОВА
Вінницький національний технічний університет

ПІДХІД ДО АНАЛІЗУ ТЕХНОГЕННОЇ ПРОБЛЕМНОЇ СИТУАЦІЇ ЯК ЗАДАЧІ ПРИЙНЯТТЯ РІШЕННЯ В УМОВАХ НЕВИЗНАЧЕННОСТІ

Розглянуто особливості організації проведення аналізу техногенної проблемної ситуації як задачі прийняття рішення в умовах невизначенності.

Features of the organization to analyze man-made problem situation as a decision problem under uncertainty have been considered.

Ключові слова: проблемна ситуація, прийняття рішень в умовах невизначенності, аналіз техногенної проблемної ситуації, оптимальне рішення, область допустимих рішень, область компромісів.

Вступ

Для ефективного вирішення задач аналізу техногенної проблемної ситуацій (ПС) доцільно розробити систему аналізу техногенної проблемної ситуації, яка функціонує в умовах невизначеності. Створення автоматизованих систем аналізу техногенних проблемних ситуацій ускладнюється за рахунок відсутності формалізованих зв'язків між об'єктами та їх ознаками, неповноти, неточності та неоднозначності вхідних даних, які частіше за все характеризуються лише якісними оцінками. В таких умовах погано формалізовані задачі не мають точного рішення і вимагають використання наближених методів, заснованих на використанні емпіричних даних, експертних оцінок, нечітких та некласичних логік, спеціально розроблених методів та моделей [1-3].

Незважаючи на активні дослідження автоматизованих систем управління на основі нечіткої логіки, все ще достатньо неповністю вирішено багато питань, пов'язаних з розробкою методів, моделей і алгоритмів виявлення експертних знань, класифікації ситуацій, формулювання управлінських рішень при нечітко заданій інформації та ін.

Тому, для підвищення ефективності функціонування систем аналізу техногенних проблемних ситуацій актуальним та важливим є розробка системи аналізу техногенної проблемної ситуації на основі нечіткої логіки.