Досліджений круг проблем, пов'язаних з застосуванням методів захисту інформації - ідентифікації та аутентифікації, які засновані на використанні переносних пристроїв, паролів, біометричних характеристик, шляхом з'ясування координат користувача, визначено переваги та недоліки розглянутих методів, перспективи їх подальшого розвитку

Ключові слова: аутентифікація, ідентифікація, пароль, біометрія, токен

Исследован круг проблем, связанных с применением методов защиты информации - идентификации и аутентификации, которые основаны на использовании переносных устройств, паролей, биометрических характеристик, путем определения координат пользователя, определены преимущества и недостатки рассмотренных методов, перспективы их дальнейшего развития

Ключевые слова: аутентификация, идентификация, пароль, биометрия, токен

УДК 614.2

ІДЕНТИФІКАЦІЯ І АУТЕНТИФИКАЦІЯ – МЕТОДИ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

З.М. Гадецька
Кандидат технічних наук, доцент*
E-mail: josi@ukr.net
Д.Г. Омельчук*
E-mail: emeildimka@mail.ru
Р.В. Литвин*
E-mail: big-litvin-roman@bigmir.net
*Кафедра комп'ютерних технологій та автоматизації процесів управління
Академія пожежної безпеки ім. Героїв Чорнобиля
вул. Правика, 8, м. Черкаси, Україна, 18034

1. Вступ

Інформація, що зберігається на комп'ютері, є інтелектуальною власністю користувача, а тому потребує захисту, як і будь-яка інша власність. Залежно від можливих порушень у роботі системи та загроз несанкціонованого доступу до інформації використовуються різні види захисту інформації, які можна об'єднати у такі групи: морально-етичні, правові, адміністративні (організаційні), технічні (фізичні), програмні. Зазначимо, що такий поділ є досить умовним. Зокрема, сучасні технології розвиваються в напрямку сполучення програмних та апаратних засобів захисту. Основою програмно-технічних засобів безпеки вважається ідентифікація і аутентифікація. Ідентифікація і аутентифікація - це перша лінію оборони, «прохідна» інформаційного простору організації або установи.

Ідентифікація – процедура розпізнавання користувача в системі як правило за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою. Даний термін звичайно означає встановлення особистості користувача. Аутентифікація – процедура встановлення належності користувачеві в системі пред'явленого ним ідентифікатора. За допомогою аутентифікації система переконується, що суб'єкт справді той, за кого себе видає [1].

Сьогодні існує декілька способів ідентифікації та аутентифікації користувачів. У кожного з них є свої переваги і недоліки, завдяки чому деякі технології підходять для використання в одних системах, інші - в інших. Однак у багатьох випадках немає строго певного рішення. А тому як розроблювачам програмного забезпечення, так і користувачам приходиться самостійно думати, який спосіб ідентифікації реалізовувати в продуктах.

2. Постановка проблеми

Кожний користувач сучасних інформаційно-комунікаційних систем декілька разів на день стикається з процедурами ідентифікації та аутентифікації. Ці процедури виконуються кожний раз, коли користувач вводить пароль для доступу до інформаційної системи, мережі, бази даних або при запуску прикладної програми. В результаті їх виконання оператор або отримує доступ до певних ресурсів інформаційної системи, або ні.

Процедура аутентифікації користувача є обов'язковим етапом функціонування будь-якої сучасної інформаційно-комунікаційної системи. Існує декілька методів ідентифікації і аутентифікації, які різняться своєю складністю, надійністю, вартістю та іншими показниками. Кожний з цих методів має свої позитивні та негативні сторони, аналізу яких присвячена ця робота.

3. Аналіз останніх досліджень і публікацій

Аналіз робіт [1-11], присвячених порівнянню відомих методів ідентифікації та аутентифікації, дозволив виявити ряд недоліків цих робіт: обмежене коло розглянутих методів, відсутність чітко визначених показників оцінки їх якості, відсутність системності

при проведенні оцінювання, відсутність, в більшості випадків, кількісних характеристик (оцінки виражені в нечіткій лінгвістичній формі), велика доля суб'єктивізму при оцінюванні зумовлена в тому числі комерційними (маркетинговими) інтересами.

4. Мета статті

Аналіз і систематизація на базі визначених показників переваг і недоліків сучасних методів аутентифікації та ідентифікації користувачів інформаційно-комунікаційних систем, визначення подальших перспектив розвитку зазначених методів.

5. Результати

Для вирішення завдання порівняльного оцінювання методів ідентифікації та аутентифікації користувачів перш за все необхідно визначитись із вичерпним переліком показників, за якими будуть оцінюватись системи аутентифікації та ідентифікації. За результатами аналізу досліджень, проведених в [1-4], запропоновано наступні показники:

1. Стійкість до перебору.
2. Захищеність від підглядання.
3. Захищеність від викрадання аутентифікатора та ідентифікатора.
4. Захищеність у разі викрадання матеріальних носіїв, на яких зберігається аутентифікатор або ідентифікатор.
5. Вартість системи аутентифікації та ідентифікації.
6. Простота запам'ятовування аутентифікатора та ідентифікатора.
7. Простота зміни аутентифікатора та ідентифікатора.
8. Простота процедури аутентифікації та ідентифікації.
10. Можливість використання аутентифікатора та ідентифікатора неуповноваженим суб'єктом.
11. Стійкість до дій зовнішніх факторів: температура, волога, механічне пошкодження.

Проведемо оцінку основних методів ідентифікації та аутентифікації користувачів за визначеними показниками.

Існує три найпоширеніших види ідентифікації [2]:

• парольна ідентифікація;

Кожен зареєстрований користувач системи одержує набір персональних реквізитів (звичайно використаються пари: логін-пароль).

• апаратна ідентифікація;

Цей принцип ідентифікації ґрунтується на визначенні особистості користувача за певним предметом, ключем (електронні ключі, проксіміті-карти, смарт-карти,магнітні карти), що перебуває в його ексклюзивному користуванні.

Методи аутентифікації умовно можна поділити на однофакторні та двофакторні. Однофакторні методи діляться на [2]:

• логічні (паролі, ключові фрази, які вводяться з клавіатури комп'ютера чи клавіатури спеціалізованого пристрою);

• ідентифікаційні (носієм ключової інформації є фізичні об'єкти: дискета, магнітна карта, смарт-карта, штрих-кодова карта тощо);

• біометричні (в їх основі - аналіз унікальних характеристик людини, наприклад: відбитки пальців, малюнок райдужної оболонки ока, голос, обличчя).

Надійна ідентифікація і аутентифікація уповільнюється низкою принципових причин. По-перше, комп'ютерна система ґрунтується на інформації в тому вигляді, в якому вона була отримана; строго кажучи, джерело інформації залишається невідомим. По-друге, майже всі аутентифікаційні відомості можна почути, вкрасти чи підробити. По-третє, є протиріччя між надійністю аутентифікації з одного боку, і зручностями користувача і системного адміністратора з іншого. Так, з міркувань безпеки необхідно з певною частотою просити користувача повторно вводити аутентифікаційну інформацію (адже на його місце мігла сісти інша людина), але це а це підвищує вірогідність підглядання за введенням. По-четверте, чим надійніший засіб захисту, тим він дорожчий.

Найбільш поширеним засобом аутентифікації є паролі. Система порівнює введений і раніше заданий для даного користувача пароль; у разі збігу справжність користувача вважається доведеною. Інший засіб, поступово набирає популярність і забезпечує найбільшу ефективність, - секретні криптографічні ключі користувачів.

Необхідно шукати компроміс між надійністю, зручністю, доступністю за ціною адміністрування на ідентифікацію і аутентифікацію. Зазвичай компроміс досягається з допомогою комбінування двох перших з вище перерахованих базових механізмів перевірки справжності.

Перелічені заходи доцільно застосовувати завжди, навіть якщо поруч із паролями використовуються інші методи аутентифікації, засновані, наприклад, на застосуванні токенів.

Токен - це предмет чи пристрій, володіння яким підтверджує справжність користувача. Токен - це компактний пристрій у вигляді USB-брелока, яке призначений для авторизації користувача, захисту електронного листування, безпечного віддаленого доступу до інформаційних ресурсів, а також надійного зберігання будь-яких персональних даних. Ці пристрої мають власну захищену пам'ять і підключаються безпосередньо до одного з портів комп'ютера (USB, LPT). Розрізняють токени з пам'яттю (пасивні, які лише зберігають, але з обробляють інформацію) і інтелектуальні токени (активні).

Найпоширенішим різновидом токенов з пам'яттю є картки з магнітною смугою. Для використання цих токенів необхідно також мати пристрій читання. Головною перевагою застосування апаратної ідентифікації є досить висока надійність. У пам'яті токенів можуть зберігатися ключі, підібрати які хакерам не вдасться. Крім того, у них реалізовано чимало різних захисних механізмів. А вбудований мікропроцесор дозволяє електронному ключу не тільки брати участь у процесі ідентифікації користувача, але й виконувати деякі інші корисні функції. Недоліком апаратної ідентифікації є висока ціна. Взагалі ж останнім часом вартість як самих токенів, так і програмного забезпечення, що може працювати з ними, помітно знизилася.

Пристрої контролю біометричних характеристик складні, і недешеві, тому вони як правило застосовуються лише у специфічних організаціях з високими вимогами до безпеки.

Останнім часом здобуває популярність аутентифікація шляхом з'ясування координат користувача. Ідея у тому, щоб користувач посилав координати супутників системи GPS (Global Positioning System), що знаходяться у зоні прямої видимості. Сервер аутентифікації знає орбіти всіх супутників, тому можна з точністю до метри визначити місцезнаходження користувача. Оскільки орбіти супутників не завжди стабільні, передбачити які дуже складно, підробка координат виявляється практично неможливою. Нічого не дає і перехоплення координат - вони постійно змінюються. Безперервна передача координат не потребує від користувача будь-яких додаткових зусиль, і тому він може легко багаторазово підтверджувати свою справжність. Апаратура GPS порівняно недорога і апробована, у тому випадку, коли легальний користувач має перебувати у певному місці, даний метод перевірки справжності є досить привабливим.

Дуже важливим і складним завданням є адміністрування служби ідентифікації і аутентифікації. Необхідно постійно підтримувати конфіденційність, цілісність і доступність відповідної інформації, що особливо непросто в мережевому різнорідному середовищі. Доцільно, поруч із автоматизацією, застосувати максимально можливу централізацію інформації. Досягти цього можливо, застосовуючи виділені сервери перевірки справжності (такі як Kerberos) чи кошти централізованого адміністрування (наприклад CA- Unicenter). Деякі операційні системи пропонують мережні сервіси, які можуть служити основою централізації адміністративних даних. Централізація полегшує роботу як системним адміністраторам, так і користувачам, оскільки це дозволяє реалізувати важливу концепцію єдиного входу. Раз пройшовши перевірку дійсності, користувач отримує доступ до всіх ресурсів мережі у межах своїх повноважень.

6. Висновки

Конкретні методи захисту інформації визначаються виробничими, фінансовими та іншими можливостями підприємства (організації), обсягом конфіденційної інформації та її значущістю. Але треба пам'ятати, що абсолютно надійного захисту просто не існує. Заходи із захисту інформації повинні мати комплексний, систематичний характер, об'єднувати різні засоби. Особливо важливо, щоб питання інформаційної безпеки потрапили в сферу особливої уваги керівників організацій та установ - без їх підтримки зробити що-небудь істотне в цій галузі неможливо.

Література

1. Грайворонський, М. В. Безпека інформаційно-комунікаційних систем [Текст] : учеб./ М. В. Грайворонський, О. М. Новіков. - К.: Видавнича група BHV, 2009. - 608 с.
2. Охота, Д. Б. Технології комп'ютерної безпеки [Текст] / Д. Б. Охота. - Рівне: МЕГУ, 2011. - 97 с.
3. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства [Текст] / В. Ф. Шаньгин . - М.: ДМК Пресс, 2008. - 544 С.
4. Шрамко, В. Н. Защита компьютеров: электронные системы идентификации и аутентификации [Текст] / В. Н. Шрамко // PCWeek/RE. - 2004. - №12.
5. Todorov Dobromir Mechanics of user identification and authentication: fundamentals of identity management [Электронный ресурс]. - Режим доступа: \www/ URL:http://www.amazon.com/Mechanics-User-Identification -Authentication-Fundamentals/dp/1420052195#reader_1420052195/.- Загл. с экрана.
6. Stephen Downes Authentication and Identification [Электронный ресурс]. - Режим доступа: \www/ http://itdl.org/Journal/Oct_05/article01.htm/. - Загл. с экрана.
7. J.D. Rollason, K.I. Munro and T.M. Addison IS Security: User Identification and Authentication with reference to South African Financial Services Case Studies [Электронный ресурс]. - Режим доступа: \http://icsa.cs.up.ac.za/issa/2002/proceedings/A022.pdf. - Загл. с экрана.
8. Mikko Lehtonen, Thorsten Staake From Identification and Authentication - A Review of RFID Product Authentication Techniques [Электронный ресурс]. - Режим доступа: \http://www.slideshare.net/ PeterSam67/from-identification-to-authentication-a-review-of-rfid. - Загл. с экрана.
9. M. E. Kabay Identification, Authentication and Authorization on the World Wide Web1 [Электронный ресурс]. - Режим доступа: \http://www.mekabay.com/infosecmgmt/iaawww.pdf. - Загл. с экрана.
10. Russell Kay QuickStudy: Biometric authentication [Электронный ресурс]. - / Computerworld.—Режим доступа: \ ttp://www.computerworld.com /s/article/100772/Biometric_Authentication. - Загл. с экрана.
11. Stephen Downes Authentication and Identification Techniques [Электронный ресурс]. - Режим доступа: \hhttp://www.downes.ca/post/12. - Загл. с экрана.