УДК 004.056.5:004.439

Франчук В.М.,
кандидат педагогічних наук, доцент,
Національний педагогічний університет імені М.П. Драгоманова

ЗАХИСТ ДАНИХ. ЗАСОБИ ПАРОЛЬНОЇ ІДЕНТИФІКАЦІЇ ТА АДМІНІСТРУВАННЯ

Анотація. У статті розглядаються засоби ідентифікації користувачів, як один із способів захисту даних в комп’ютерних системах. Існує кілька способів ідентифікації користувачів: апаратна, біометрична, парольна, багатофакторна. У кожного способу ідентифікації є свої переваги і недоліки, завдяки чому деякі технології придатні для використання в одних системах, інші - в інших. Засоби парольної ідентифікації користувачів є найбільш поширеними, тому у статті більш детальніше описано використання та створення надійних паролів та їх адміністрування.

Ключові слова: захист даних, апаратна ідентифікація, біометрична ідентифікація, парольна ідентифікація, багатофакторна ідентифікація.

В сучасному світі, в якому велика кількість видів діяльності людей супроводжується комп'ютерною підтримкою, проблема безпеки комп'ютерних систем є надзвичайно актуальною. Врахування усіх недоліків захисних механізмів, передбачення можливих наслідків та загроз безпеки інформаційних ресурсів може убезпечити комп'ютерних користувачів від небажаних впливів різноманітних обставин і сторонніх людей на їхнє життя. Саме тому в наш час користувачам потрібно володіти навичками використання апробованих методів і надійних засобів захисту комп'ютерних даних та розумітися у проблемі захисту інформаційних ресурсів в усій її багатогранності [1].

Одним із способів захисту даних в комп’ютерних системах є ідентифікація користувачів. Ідентифікація в інформаційній безпеці – процедура розпізнавання користувача в системі, як правило, за допомогою наперед

визначеного імені (ідентифікатора) або інших апріорних даних про нього, які сприймаються за допомогою системи [2].

Ця процедура необхідна для того, щоб за допомогою системи надалі можна ухвалити рішення щодо подання людині дозволу для роботи на комп'ютері, доступу до закритих даних і т.д. Таким чином, ідентифікація є одним з основних понять в інформаційній безпеці.

Сьогодні існує кілька способів (видів) ідентифікації користувачів. У кожного з них є свої переваги і недоліки, завдяки чому деякі технології придатні для використання в одних системах, інші - в інших.

Однак у багатьох випадках немає строго певного рішення. А тому як розробникам програмного забезпечення, так і користувачам доводиться самостійно обирати, який спосіб ідентифікації реалізовувати в цих програмних засобах.

Розглянемо детальніше способи ідентифікації облікових записів користувачів у комп’ютерних системах.

Апаратна ідентифікація. Цей вид ідентифікації ґрунтується на визначенні облікового запису користувача за якимось предметом, ключем, що перебуває в його ексклюзивному користуванні. Мова йде не про звичайні, звичні для більшості людей ключі, а про спеціальні електронні. На даний момент найбільшого поширення одержали два типи пристроїв. До першого відносяться всілякі карти. Їх досить багато, і використовуються вони за різними принципами. Так, наприклад, досить зручні у використанні безконтактні карти, за допомогою яких користувачі можуть проходити ідентифікацію як у комп'ютерних системах, так і в системах доступу в приміщення. Найбільш надійними вважаються смарт-карти – аналоги звичних багатьом користувачам банківських карт. Крім того, є й більш дешеві, але менш стійкі до злому карти: магнітні, зі штрих-кодом і т. д. (Рис. 1).

Рис. 1

У цих пристроїв досить досконалі характеристики надійності. У них вбудований мікропроцесор (чіп), за допомогою якого можна реалізувати різні алгоритми захисту.

Залежно від виробника захищеність смарт-карт може змінюватися. Крім цього у них можуть вбудовуватися різні датчики, призначення яких – заборона функціонування мікропроцесора (чіпа) в разі спроби пошкодження пластика. Це можуть бути температурні датчики або датчики, «чутливі» до механічних впливів – наприклад, до зрізання пластикового впакування для прямого доступу до електроніки. Всі дані, що зберігаються в чіпі, шифруються, щоб фахівцю, який знайде вразливість до вмісту мікросхеми не вдалося її «прочитати», принаймні відразу. Є також захист від підбирання пароля аж до знищення всіх даних, що знаходяться в чіпі. Також смарт-карти призначені для зберігання персональних даних, паролів доступу і даних для ідентифікації. Для успішної ідентифікації потрібно вставити смарт-карту у зчитувальний пристрій і ввести пароль (PIN-код).

Іншим типом ключів, які можуть використовуватися для апаратної ідентифікації, є токени. У ці пристрої вбудована захищена пам'ять і під’єднуються безпосередньо до одного з портів комп'ютера (USB, LPT) (Рис. 2).

Рис. 2

Що стосується USB-токенів, то зовні цей пристрій виглядає як звичайний USB-накопичувач (флешка), але за своїм функціональним призначенням багато в чому відповідає смарт-карті. Користуватися цими пристроями зручно, оскільки немає необхідності запам'ятовувати різні паролі і коди доступу, всі дані зберігається в USB-токені. Крім того на носієві можуть бути записані цифрові підписи, сертифікати й інші дані, які небезпечно зберігати на жорсткому диску комп’ютера.

Процес двохфакторної ідентифікації з використанням USB-токенів проходить у два етапи: користувач під’єднує цей пристрій через USB-порт комп'ютера і вводить PIN-код. Перевагою цього способу ідентифікації є висока мобільність, тому що USB-порти є у кожному комп’ютері. Застосування окремого фізичного пристрою дозволяє забезпечити безпечне зберігання конфіденційних даних (ключів шифрування, цифрових сертифікатів тощо), реалізувати безпечний локальний або віддалений вхід в обчислювальну мережу, шифрування файлів на пристроях зберігання даних на робочих станціях і серверах, управління правами користувача і здійснення безпечних транзакцій.

Головною перевагою застосування апаратної ідентифікації є досить висока надійність, окільки, у пам'яті токенів можуть зберігатися ключі, підібрати які неможливо. Крім того, у них реалізовано чимало різних захисних механізмів. А використання вбудованого мікропроцесора дозволяє використовувати електронний ключ не тільки у процесі ідентифікації користувача, але й для виконання деяких інших корисних функцій. Найбільш серйозною небезпекою у випадку використання апаратної ідентифікації є крадіжки зловмисниками токенів у зареєстрованих користувачів. Втім, ця проблема легко вирішується за допомогою застосування багатофакторної ідентифікації (про те, що це таке, буде сказано нижче).

Що стосується недоліків – це можливість крадіжки електронних ключів. Другий недолік розглянутої технології – вартість. Разом з тим останнім часом вартість як самих електронних ключів, так і програмного забезпечення, що

може використовуватися з ними, помітно знизилася. Проте для введення в експлуатацію системи апаратної ідентифікації однаково будуть потрібні деякі вкладення. Все-таки кожного зареєстрованого користувача (або хоча б привілейованих користувачів – адміністраторів, керівництво підприємства і т.д.) потрібно забезпечити персональними токенами. Крім того, згодом деякі типи ключів можуть зношуватися, крім того, вони можуть бути загублені і т.д. Тобто використання апаратної ідентифікації вимагає деяких експлуатаційних витрат.

Біометрична ідентифікація. Біометрія – це ідентифікація людини за унікальними, властивим тільки їй біологічним ознакам. Біометричні технології здавна розроблялися для точного встановлення особистості людини. А тому використання їх для забезпечення інформаційної безпеки виглядає цілком логічним. Причому цей напрямок розвивається дуже активно. Сьогодні використовується вже більше десятка різних біометричних ознак. Причому для найпоширеніших з них (відбитки пальців і райдужна оболонка ока) існує безліч різних за принципом дії сканерів (Рис. 3).

Рис. 3

Головною перевагою біометричних технологій є найвища надійність, оскільки двох людей з однаковими відбитками пальців у природі просто не існує. Разом з тим, сьогодні вже відомо кілька способів «обману» дактилоскопічних сканерів. Наприклад, потрібні відбитки пальців можуть бути перенесені на плівку або до пристрою може бути прикладена велика фотографія пальця зареєстрованого користувача.

Основним недоліком біометричної ідентифікації є вартість устаткування. Адже для кожного комп'ютера, що входять до цієї системи, необхідно придбати власний сканер. Останнім часом з'явилися маніпулятори типу «мишки» й

клавіатури з убудованими дактилоскопічними сканерами. Причому їхня ціна ненабагато відрізняється від вартості «звичайної» периферії. Але, слід зауважити, що подібні дешеві сканери недовговічні. Крім того, у них досить високий відсоток помилок другого роду (відмова в доступі зареєстрованому користувачеві).

Багатофакторна ідентифікація. В розглянутих попередніх системах для визначення користувача використовувався тільки один фактор (однофакторна ідентифікація). Однак подібні процеси не можна назвати надійними. Наприклад, зловмисник може вкрасти токен у зареєстрованого користувача й легко скористатися ним для несанкціонованого доступу до даних. Саме тому поступово все більшого поширення набуває багатофакторна ідентифікація, коли для визначення облікового запису користувача застосовується відразу кілька параметрів (факторів).

Причому комбінуватися ці фактори можуть у довільному порядку (Рис. 4). Втім, сьогодні в переважній більшості випадків використовується тільки одна пара: парольний захист (див. далі) і токен (у деяких випадках може використовуватися номер мобільного телефону).

Рис. 4

У цьому випадку використання паролю без електронного ключа буде безрезультатним, як і використання токена без паролю. Разом з тим, у деяких системах застосовуються максимально надійні процедури ідентифікації. У них одночасно використовуються паролі, токени й біометричні характеристики людини.

Парольна ідентифікація. Ще не дуже давно парольна ідентифікація була ледве не єдиним способом визначення облікового запису користувача. Справа в тому, що парольна ідентифікація найбільш проста як у реалізації, так і у використанні.

Суть її зводиться до наступного. Кожен зареєстрований користувач якої-небудь системи одержує набір персональних реквізитів (звичайно використається пара логін-пароль). Далі у кожній спробі входу користувач повинен вказати свої дані (Рис. 5). Але оскільки вони унікальні для кожного користувача, то відповідно у системі відбувається ідентифікація облікового запису користувача.

Рис. 5

Головна перевага парольної ідентифікації – це простота реалізації й використання. Крім того, введення парольної ідентифікації не вимагає зовсім ніяких витрат: даний процес реалізований у всіх програмних продуктах, що є в продажу. Таким чином, система захисту даних виявляється гранично простою і доступною.

Разом з тим головний недолік – залежність надійності ідентифікації від самих користувачів, точніше, від обраних ними паролів. Справа в тому, що часто користувачі використовують ненадійні ключові слова, які легко розгадати. Зокрема до них відносяться занадто короткі паролі. Тому деякі фахівці в галузі інформаційної безпеки радять використовувати довгі паролі, що складаються з довільного набору букв, цифр і різних символів.

Засоби парольної ідентифікації користувачів дуже поширені. Вони використовуються практично скрізь: і в операційних системах, і в програмних додатках, і в сервісах комп’ютерних мереж.

Наприклад, для встановлення паролю на запуск операційної системи персонального комп'ютера можна скористатись спеціальними засобами зміни установок у CMOS Setup. Разом з тим, використання подібної парольної ідентифікації не є надійним. Ще не дуже давно досить було ввести універсальний пароль чи від'єднати акумуляторну батарею, розташовану на материнській платі, чи за наявності перемикача скидання пароля BIOS реалізувати це скидання, чи реалізувати коротке замикання батареї і в комп'ютері, щоб анулювалися всі установки CMOS Setup. Однак, розробники усувають подібні можливості ще й тому, що є багато програм, за допомогою яких легко зламуються такі паролі.

В системі *Windows* також передбачені різноманітні системи захисту, хоч ця операційна система спроектована як засіб підтримки роботи багатьох користувачів, а не як система захисту. Тим не менш, в ній є компоненти для забезпечення певної системи безпеки. Крім парольного захисту при вході в систему можна, наприклад, встановити пароль екранної заставки чи мережевий захист файлів та папок.

В операційних системах **nix* ще не так давно відомості про пароль будь-якого користувача можна було відшукати у файлі passwd, що знаходився в каталозі etc. Ці дані подавались у зашифрованому вигляді через двокрапку відразу після імені відповідного користувача. Але в разі доступу до парольного файлу *Unix,* можна скопіювати цей файл на окремий комп'ютер і потім скористатись однією з програм для зламування захисту *Unix.*

З часом базу паролів *nix перенесли у «затінений» режим (в каталог etc/shadow), у якому нею зміг би скористатись лише адміністратор (root, користувач з найширшими повноваженнями). До того ж дані там зашифровані за алгоритмом MD5.

В *Unix* також застосовуються різні способи шифрування облікових записів, зокрема htppasswd-файлів. В них містяться бази web-аутентифікації за допомогою web-сервера Apache (найчастіше тут використовується алгоритм

DES). В *Linux*-системах також може використовуватися CFS – криптографічна файлова система і TCFS – прозора криптографічна файлова система.

Після введення парольного захисту почали з'являтись спеціальні програми, використання яких дозволяє цей захист долати. За такими програмами здійснюється як прямий добір паролів, так і пошук за словником, а також використовуються різноманітні комбіновані методи (коли, наприклад, в якості словника використовується файл із заздалегідь обчисленими хешованими паролями).

Різноманітні парольні зломщики для системних адміністраторів є цінним інструментом, за допомогою яких можна виявляти слабкі місця парольного захисту операційних систем. Знаючи ці слабкі місця, можна відповідно налаштувати систему захисту. В основному – це обмеження фізичного доступу до конкретних каталогів і ресурсів, додаткове шифрування та підвищення вимог до паролів користувачів.

Способи захисту паролів. Найпопулярніший спосіб захисту від перебирання паролів — блокування входу на сервіс після кількох невдалих спроб. В цьому випадку неможливо нормально перебирати паролі. Але всі відомі брутфорсери (Brute Forcer) «уміють» використовувати проксі-сервери, за допомогою яких вони здійснюють перебирання. Блокування за IP-адресами в цьому випадку просто втрачає сенс. Отже лише блокуванням домогтися повноцінного захисту важко.

Останнім часом швидко поширюється в Інтернет спосіб, за яким динамічно генеруються картинки (в основному, форматів png та jpg) з кодом. І коли в разі входу на сервіс вводиться логін, користувачеві пропонується ввести код, який він бачить на картинці. «Розкрити» картинку і знайти в ній цифри досить не просто. Для цього доводиться писати складний аналізатор зображення. Значно ускладнює таке розкривання використання додаткових фонових зображень і нестандартних шрифтів.

Існують спеціальні генератори паролів, що спрощують процес добирання паролів. Такі програми постійно вдосконалюються. Наприклад, розробник

сучасного генератора випадкових паролів для *Linux* – програми *GPW,* врахував умову вимовності під час генерування парольних фраз (щоправда, лише англомовних). Тепер для захисту облікового запису в усіх версіях *Debian GNU/Linux* і *Ubuntu,* поштової скриньки, особистих даних і для створення особистих ключів WI-FI можна скористатися будь-яким вимовним паролем довжиною до 99 символів, згенерованим за допомогою цієї програми.

Часто процедури генерування паролів входять у функції парольних програм-менеджерів, за якими усі паролі користувача (або багатьох користувачів) систематизуються, шифруються і надійно зберігаються. Існують і програмно-апаратні комплекси, виконані на основі USB-ключів чи смарт-карт, за допомогою яких проблема зберігання паролів вирішується на користь мобільності.

Для того, щоб підвищити «непробивність» свого паролю, потрібно використовувати кілька способів. По-перше, різні перестановки слів, включаючи заміну першої літери на прописну, заміну всіх літер на прописні, інверсія слова, заміна літери O на цифру 0, літери I на цифру 1 (або на знак оклику), заміна літери S на цифру 5, перетворення в множину (house-houses). Цей спосіб дає близько 1000000 варіантів для перебирання.

По-друге, різні перестановки слів, що не перекривають перший спосіб, заміна однієї малої літери на прописну (Olexander, oleXander, olexaNder та ін.), заміна двох (трьох і т.д.) малих літер (OlexaNder, OleXanDer). Другий спосіб за умови заміни однієї літери дає 400 000 варіантів, 2-х – 1 500 000 варіантів, 3-х 3 000 000 варіантів для їх перебирання.

Найбільш складний і захищений варіант – це пароль, що складається з двох коротких слів зі знаком пунктуації між ними. Пароль, що складається з двох слів довжиною від 3 до 5 символів і знаку пунктуації між ними, дає близько 90 000000 варіантів для перебирання (і це без використання першого та другого способів).

Літери, цифри, метасимволи ?, !, $, @, #, пробіли. Однак оскільки в деяких додатках «обрізаються» пробіли, краще не починати і не закінчувати

пароль пробілом. Використання пробілів полегшує користувачам створення більш складних паролів. Оскільки пробіл може вставлятися між словами, це може дати реальну можливість використовувати довгі паролі з кількох слів.

У деяких випадках у паролях можна використовувати символи з великим ASCII-кодом для додаткового ускладнення пароля. Ці символи не можуть бути природним чином набрані на клавіатурі, але вводяться з утриманням кнопки ALT і набором ASCII-коду на цифровій клавіатурі. Дуже корисним у паролях може виявитись нерозривний пробіл (ALT+0160). Цей символ відображається як звичайний пробіл і найчастіше може ввести в оману тих, хто якимось чином підгледів пароль. І навіть встановлений кейлогер (шпигунський програмний засіб призначений для запису послідовності використаних клавіш клавіатури) у створюваному файлі нерозривний пробіл буде записаний у вигляді звичайного пробілу [1].

Фахівці радять також в якості паролів (чи їх частин) добирати фрази, набір яких на клавіатурі потребує чергування клавіш лівої та правої рук (це збільшить швидкість набирання, скоротить кількість помилок і зменшить шанс того, що хто-небудь зможе підглянути пароль, спостерігаючи за рухами пальців під час його введення).

Краща техніка для створення складних паролів, що однак легко запам'ятовуються – використання структур, які звик запам'ятовувати користувач. Такі структури можуть містити телефонні номери, адреси, імена, шляхи до файлів і т.д. Можна також використовувати різні шаблони, повторення, рими, гумор, сленг, жаргон і т. ін.

Ідеального захисту даних немає. Але все-таки слід зазначити, що, скориставшись перерахованими вище способами, можна досягти досить високого ступеня захищеності даних на персональному комп’ютері.

Список використаних джерел

1. Смалько О.А. Захист інформаційних ресурсів: Монографія. - Кам’янець-Подільський: ПП Буйницький О А, 2011. - 704 с.

2. Ідентифікація (інформаційна безпека). [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Ідентифікація_(інформаційна_безпека).

В.М. Франчук

ЗАЩИТА ДАННЫХ. СРЕДСТВА ПАРОЛЬНОЙ ИДЕНТИФИКАЦИИ И АДМИНИСТРИРОВАНИЯ

Аннотация. В статье рассматриваются средства идентификации пользователей, как один из способов защиты данных в компьютерных системах. Существует несколько способов идентификации пользователей: аппаратная, биометрическая, парольная, многофакторная. У каждого способа идентификации есть свои преимущества и недостатки, благодаря чему некоторые технологии подходят для использования в одних системах, другие в иных. Средства парольной идентификации пользователей является наиболее распространенными, поэтому в статье более подробно описано использование и создание надежных паролей и их администрирования.

Ключевые слова: защита данных, аппаратная идентификация, биометрическая идентификация, парольная идентификация, многофакторная идентификация.

V.M. Franchuk

DATA PROTECTION. MEANS PASSWORD IDENTIFICATION AND MANAGEMENT

Resume. In the article considers the means of identification of users as one way to protect data in computer systems. There are several ways to identify users, hardware, biometric, levels of password, multifactor. Each method of identification has its advantages and disadvantages, so some technologies are suitable for use in some systems, the other in the other. Means password user identification are the most widespread, so the article is more details describes how to use and creation of strong passwords and their administration.

Keywords: data protection, hardware identification, biometric identification, levels of password identification, multifactor identification.