УДК 656.212.5:581.3

Д. О. ОСТАПЕЦЬ, В. ЛАПІН (ДІІТ)

РОЗРОБКА ТА ДОСЛІДЖЕННЯ КОМПЛЕКСУ ІДЕНТИФІКАЦІЇ / АУТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Розглянута організація підсистем ідентифікації / аутентифікації в інформаційних системах, виконано аналіз їх недоліків. Показана доцільність використання систем генерації одноразових паролів. Описане програмне забезпечення комплексу генерації одноразових паролів, проведене дослідження його характеристик (часового вікна та вимог до апаратної бази).

Рассмотрена организация подсистем идентификации / аутентификации в информационных системах, выполнен анализ их недостатков. Показана целесообразность использования систем генерации одноразовых паролей. Описано программное обеспечение комплекса генерации одноразовых паролей, проведено исследование его характеристик (временного окна и требований к аппаратной базе).

The identification / authentication subsystem architecture of information systems is considered; the analysis of their demerits is done. Advisability of using the onetime passwords generation systems is shown. The software complex of onetime passwords generation is described; the research of their characteristics (the time window and hardware requirements) is performed.

Сьогодні все більшого значення набувають питання інформаційної безпеки. Електронні способи ідентифікації людини, застосовувані в системах забезпечення санкціонованого допуску до матеріальних і інформаційних ресурсів, одержали в цей час широке поширення. Існують декілька відмінних принципів ідентифікації та аутентифікації користувачів. У кожного з них є свої переваги й недоліки, тобто немає єдиної технології для використання в усіх системах. Тому перед розроблювачами програмного та апаратного забезпечення встає питання вибору способу ідентифікації. Дана робота присвячена розробці та дослідженню комплексу ідентифікації користувачів інформаційних систем (ІС).

СПОСОБИ, МЕТОДИ ТА ЗАСОБИ ІДЕНТИФІКАЦІЇ ТА АУТЕНТИФІКАЦІЇ

Кожен користувач ІС повинен ідентифікувати себе. Звичайний спосіб ідентифікації - уведення імені користувача при вході в систему. У свою чергу, система повинна перевірити дійсність особистості користувача, тобто що він є саме тим, за кого себе видає. Аналізуючи засоби ідентифікації та аутентифікації можна виділити три основних способи ідентифікації. В основному [1, 2, 3] способи ідентифікації класифікують за факторами, що використовуються для ідентифікації (рис. 1).

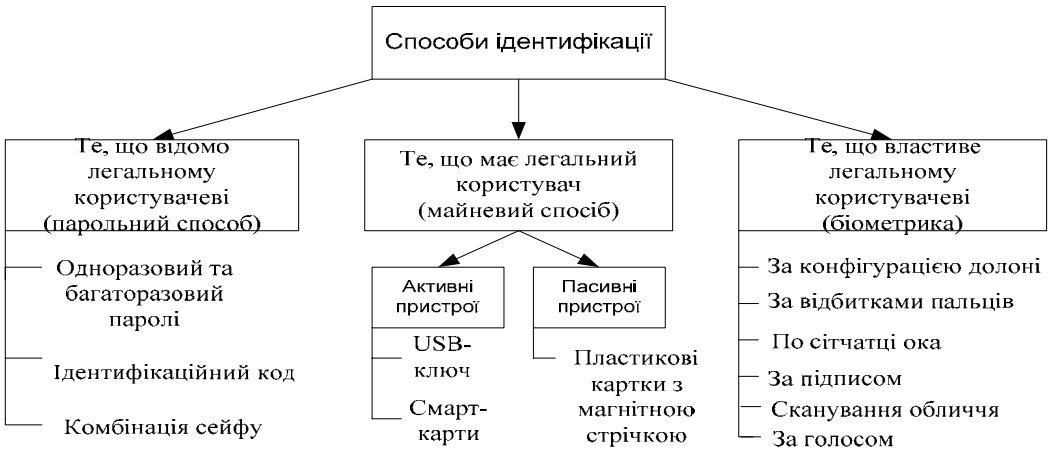

Рис. 1. Класифікація способів ідентифікації та аутентифікації в ІС

Останнім часом більшу популярність одержав біометричний спосіб ідентифікації. Майнова ідентифікація з використанням активних пристроїв – основний конкурент біометричному способу за стійкістю.

Парольний і майновий спосіб з використанням пасивних пристроїв у цей час мають найбільше поширення завдяки своїй низькій вартості. Саме цей фактор і є вирішальним у багатьох ІС, де не потрібна особлива стійкість. Більшого поширення одержує багатофакторна ідентифікація, коли для визначення особистості застосовується відразу декілька способів. Такий метод ідентифікації дає велику стійкість і при цьому витрати на його реалізацію мінімальні (наприклад, пластикова картка, яка поєднує в собі парольну та майнову ідентифікації; при цьому користувач повинен фізично мати таку картку і знати *PIN*-код для її застосування).

Узагальнене порівняння способів ідентифікації (на основі даних [4, 5]) наведено в табл. 1.

Таблиця 1

Порівняння способів ідентифікації

Способи ідентифікації / Параметри порівняння	Парольний	Майновий		Біометричний
		Активні пристрої	Пасивні пристрої	
Необхідність запам'ятовування пароля	+	–	+	–
Необхідність спеціальних апаратних засобів	–	+	+	+
Можливість помилки введення інформації користувачем	+	–	–	–
Можливість помилки системи при ідентифікації	–	–	–	+
Відносна стійкість до злому	низька	висока	середня	висока
Відносна питома вартість (на одного користувача)	низька	висока	середня	висока

З розглянутих вище способів найкраще співвідношення ціна/якість має парольний спосіб (за умови використання одноразових паролів). Саме цей спосіб обрано авторами для подальшого дослідження.

РОЗРОБКА ВНУТРІШНЬОЇ АРХІТЕКТУРИ КОМПЛЕКСУ ІДЕНТИФІКАЦІЇ

Для генерації одноразових паролів найчастіше застосовуються апаратні генератори, кожен з яких окремо початково настроєний. Такі пристрої несуть у собі базовий секрет, засоби для відліку часу або лічильник, а також засоби для хешування або шифрування [1]. В якості ключа шифру використовується базовий секрет, а в якості блоку даних, що хешується (шифрується) – показання годинника або лічильника, що налаштовується (які, наприклад, ведуть відлік часу з деякого моменту ініціалізації пристрою або кількості спроб авторизації, відповідно). Дані годинник або лічильник повинні бути синхронізовані з аналогічним серверним годинником або лічильником. Початкову синхронізацію виконує адміністратор сервера.

В апаратній реалізації таких пристроїв звичайно застосовується мікросхема, що робить хешування (шифрування) за допомогою блочного алгоритму *DES* [1]. При програмній реалізації можна використовувати і інші алгоритми хешування або блочні шифри. Такими алгоритмами, на думку авторів, можуть бути *MD5, DES, AES,* ГОСТ 28147-89. В результаті порівняння та аналізу алгоритмів хешування (шифрування) [4, 5, 6, 7] для реалізації системи обрано шифр *DES,* що відповідно до стандартів *ANSI X*9.9, *ANSI X*9.19, *ISO* 8730, *ISO* 8731-1:1987 є алгоритмом формування хеш-функцій у системах аутентифікації [2]. Даний шифр виступав як федеральний стандарт США з 1977 року по грудень 2001 року [8]. Також в даному шифрі розмір блоку даних становить 64 біта, що цілком достатньо для розв'язуваного завдання.

Після хешування (шифрування) на виході відповідного блоку ми маємо пароль у вигляді символьної або числової послідовності. Залежно від настроювання внутрішнього годинника або лічильника даний пароль динамічно змінюється через певні інтервали часу. Зміна відбувається внаслідок того, що блок даних, який ши-

фрується, на вході постійно змінюється, а функція хешування забезпечує при найменшій зміні вхідних даних на виході утворювати кардинально різні послідовності, які не піддаються певним закономірностям.

Апаратна реалізація генератора одноразових паролів тягне за собою чималі грошові витрати, тому що кожен користувач інформаційної системи повинен мати даний пристрій, який коштує близько сотень доларів [1]. Тому даний пристрій має сенс реалізувати програмно, при цьому кожен користувач буде мати свою копію даної програми та набір конфігураційних файлів, де будуть зберігатися унікальні настроювання. Все це можна зберігати на носії інформації, наприклад, флеш-накопичувачі. Таким чином, одержуємо вже двохфакторну систему ідентифікації / аутентифікації.

Комплекс складається із двох частин – клієнтської та серверної. Основним призначенням створюваного програмного продукту є використання у навчальних цілях та дослідженні, тому клієнтська та серверна частини матимуть деякі особливості та спрощення. Клієнтська частина (далі клієнт) буде перебувати у користувача і являтиме собою генератор одноразових паролів. Серверна частина (далі сервер) являє собою користувальницький інтерфейс, куди вводиться логін і одноразовий пароль користувача та на підставі перевірки пароля дозволяється або забороняється доступ до інформаційної системи.

Для забезпечення більшої безпеки при побудові ключа вводиться запит на введення *PIN*-коду, що разом з базовим секретом і дасть ключ для функції хешування.

Отримана в результаті схема клієнтської частини комплексу ідентифікації користувачів інформаційних систем представлена на рис. 2.

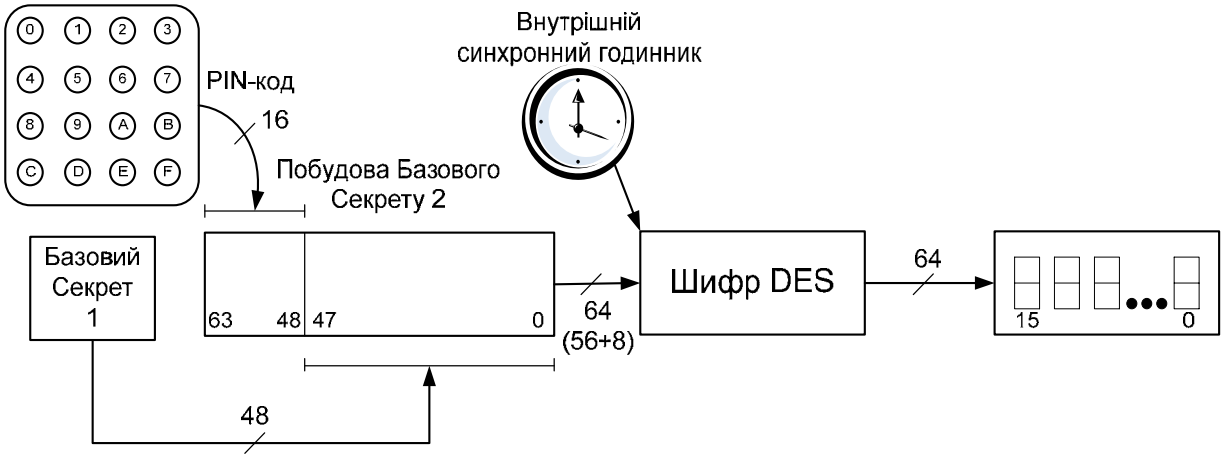

Рис. 2. Клієнтська частина комплексу ідентифікації користувачів ІС

Тут на підставі *PIN*-коду й базового секрету 1 будується ключ (базовий секрет 2) і за допомогою його відбувається шифрування блоку даних (показань внутрішнього годинника). У результаті одержуємо одноразовий пароль, який для зручності представлений у шістнадцятирічному вигляді.

В якості алгоритму шифрування був обраний шифр *DES*, який припускає розмір блоку й ключа 64 біта, а тому розрядності базового секрету 2 і показань внутрішнього годинника повинні відповідати даному числу. Настроювання внутрішнього годинника робить адміністратор системи і синхронізує його із внутрішнім годинником сервера Також адміністратор видає користувачеві базовий секрет 1.

Таким чином, розрядність *PIN*-коду обрано рівним 16 біт (4 шістнадцятирічних цифри), а розрядність базового секрету № 1 – 48 біт (12 шістнадцятирічних цифр). Показання внутрішнього годинника зберігаються у вигляді внутрішньої змінної, що становить 8 байт, тобто 64 біта блоку даних, що шифрується. На виході одержуємо пароль розрядністю 64 біта (відповідно до шифру *DES*), а це становить 16 шістнадцятирічних цифр.

Серверна частина комплексу будується аналогічно клієнтській, за винятком того, що на сервері в базі даних зберігається вже сформований базовий секрет 2 користувачів.

Схема серверної частини комплексу ідентифікації користувачів інформаційних систем представлена на рис. 3.

До складу серверної частини, як видно з рис. 3, входить база даних користувачів. База даних містить в собі логін і вже сформований базовий секрет 2 кожного користувача, а також початкове настроювання внутрішнього годинника для кожного користувача.

Користувач сам вибирає собі логін і *PIN*-код, які адміністратор вносить до бази даних.

Логін	БС2=PIN+БС1	Початкова настройка годинника
Johnny	AE23e2d76510bf24	06.05.2007 21:24:30
Serg	EABF458937aefdb2	01.02.1995 23:02:15
Sasho	56FE75fedba54081	04.05.2007 12:05:31
SvaySS	78FD64fde38a21bc	21.09.2000 17:13:12
mtkolya	ED7240deba345612	14.12.1985 18:00:00

Рис. 3. Серверна частина комплексу ідентифікації користувачів ІС з можливим варіантом бази

Робота сервера відбувається в такий спосіб. При введенні логіну та одноразового пароля в сервер відбувається вибірка з користувальницької бази даних за логіном особистих даних користувача: базового секрету 2 і початкової настройки внутрішнього годинника, які потім беруть участь у шифруванні. Шифрування відбувається при різних показаннях внутрішнього годинника з деяким значення часового вікна, яке вводиться для того, щоб користувач встиг ввести згенерований пароль. Сервер генерує всілякі комбінації пароля в рамках часового вікна і підряд порівнює їх з уведеним користувачем паролем. Якщо відбувся збіг паролів, то пароль уважається коректним і користувачеві надається доступ до інформаційної системи, у противному випадку доступ відхиляється. Користувач повинен увести згенерований пароль у рамках часового вікна, інакше пароль також буде вважатися некоректним і доступ буде відхилений.

ПРОГРАМНА РЕАЛІЗАЦІЯ КОМПЛЕКСУ

Для програмної реалізації комплексу було використано середовище *Delphi*. Правильність роботи шифру *DES* перевірялася за допомогою спеціальної функції *CryptHashData* бібліотеки *CryptoAPI*. Для цього брався деякий блок даних, який спочатку шифрувався за допомогою розробленої програми, а потім за допомогою функції *CryptHashData* і перевірялись вихідні дані.

Екранні форми клієнтської та серверної частин наведені на рис. 4 та 5.

Для роботи комплексу в клієнтській частині програми повинні бути два конфігураційних файли *bs1.txt* і *bs3.txt* з особистими настроюваннями користувача. У *bs1.txt* утримується 16-бітне число в шістнадцятирічному виді (наприклад, *AE23*), в *bs3.txt* перебуває дата-час (наприклад, 06.05.2007 21:24:30). У серверній частині комплексу повинен перебувати файл бази даних користувачів *database.txt* наступного виду (можливо декілька записів):

Лапин_Е.В. *Johnny AE23e2d76510bf24* 06.05.2007 21:24:30

Розглянемо роботу комплексу на прикладі користувача з логіном *Johnny*. Уводимо *PIN*-код *AE23* і одержуємо згенерований одноразовий пароль, нижче якого виводяться особисті дані користувача. Натиснувши на кнопку «Расшифровать», переконуємося в правильності роботи функції шифрування. На рис. 4 зображене вікно клієнтської частини програми в дії.

Рис. 4. Вікно клієнтської частини комплексу в дії

При роботі клієнтської частини комплексу відбувається зчитування конфігураційних файлів *bs1.txt* і *bs3.txt*, де зберігаються Базовий Секрет 1 і початкове настроювання внутрішнього годинника відповідно користувача з логіном *Johnny*.

Уводимо логін і одноразовий пароль у серверну частину комплексу в рамках заданого часового вікна 20 с і переконуємося, що сервер дозволяє доступ у систему користувачеві (рис. 5).

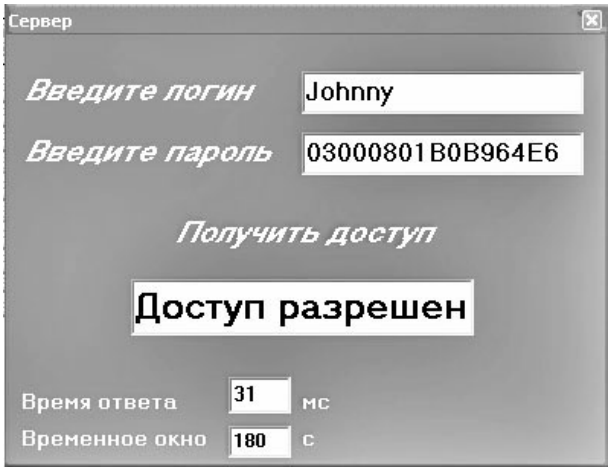

Рис. 5. Сервер дозволяє доступ користувачеві

Тепер перевіримо коректність пароля через 3 хв 30 с. Переконуємося, що сервер забороняє користувачеві доступ до системи (рис. 7).

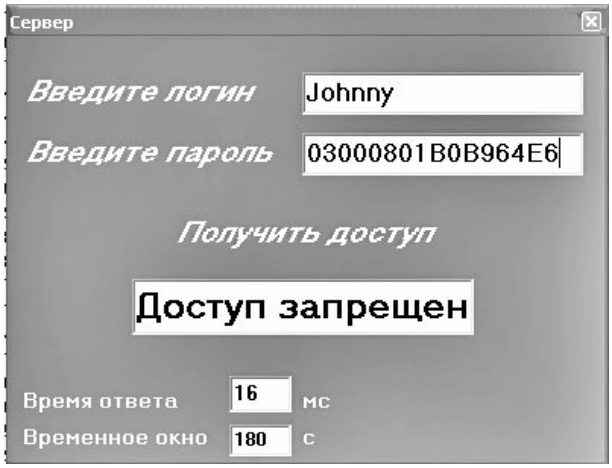

Рис. 6. Сервер забороняє доступ користувачеві

ДОСЛІДЖЕННЯ ДОПУСТИМОЇ ВЕЛИЧИНИ ЧАСОВОГО ВІКНА

Зробимо розрахунок необхідної продуктивності центрального процесору (ЦП) для забезпечення розумного часу видачі відповіді про дозвіл доступу. Розрахунок будемо робити для ситуації, коли доступ намагається отримати один користувач.

Відповідно до вихідного тексту програмного коду, для реалізації одного циклу шифрування за алгоритмом *DES* необхідно виконати $N = 8232$ коротких операцій (додавання, бітові операції тощо). Приймемо, що кожна коротка операція, в середньому, займає 2 такти центрального процесору.

Згідно [9] середній час, що потрібен для уведення та передачі згенерованого пароля користувачем складає не більше 3 хв. Таким чином, часове вікно складає 180 с, тобто ЦП повинен виконати $M = 180$ перевірок одноразового пароля (з урахуванням того, що інтервал внутрішнього годинника складає 1 с). Розрахуємо частоту ЦП, що потрібна для забезпечення часу відповіді не більше $t_O = 1$ с. Частоту ЦП можна розрахувати за формулою:

$$f = 1/T, \qquad (1)$$

де T – час виконання такту.

Значення t_O розраховується за формулою:

$$t_o \le M \times N \times \tau, \qquad (2)$$

де τ – час виконання короткої операції.

Звідти, в граничному випадку:

$$\tau = t_o /(M \times N). \qquad (3)$$

Враховуючи, що кожна коротка операція складається з 2 тактів, маємо:

$$T = \tau / 2 . \quad (4)$$

Таким чином, одержуємо кінцеву формулу для розрахунку потрібної частоти ЦП:

$$f = 2 / \tau = 2 \times M \times N / t_{\text{o}} . \quad (5)$$

Підставивши значення величин у формулу (5), отримуємо:

$$f = 2963520 \text{ Гц} . \quad (6)$$

Згідно формули (6), потрібна частота ЦП складає 2,96 МГц. Тобто, це є дуже малою величиною, сучасні комп'ютери обладнанні ЦП з частотою на порядок більше.

Проводячи тестування програми на комп'ютері з ЦП *AMD Sempron* 3200+ частотою 1,6 ГГц, виявлено, що для забезпечення часу відповіді сервера в 1 с, величина часового вікна становить приблизно 32000 с, тобто майже 9 годин. За такий час кожен користувач зможе ввести пароль.

Досвідченому користувачу для введення пароля вистачить близько 10 секунд, тому автори рекомендують встановлювати величину часового вікна 20-30 с. Це також зменшить навантаження на серверну частину системи при генеруванні паролів.

ЗАКЛЮЧНА ЧАСТИНА

Пакет програм, що розроблений в рамках даної роботи, може бути використаний в учбовому процесі або як демонстраційний засіб. Він може використовуватись в курсі «Методи та засоби захисту інформації» (спеціальність «Захист інформації в комп'ютерних системах та мережах») при вивченні методів та засобів ідентифікації та аутентифікації. За допомогою даного пакету програм можуть бути вивчені (продемонстровані):

- загальні уявлення про ідентифікацію / аутентифікацію за допомогою одноразових паролів;
- шифрування за алгоритмом *DES*;
- вплив величини часового вікна на продуктивність роботи системи та відмови в обслуговуванні користувачів;
- розрахунки кількісних величин (величина часового вікна, вимоги до апаратної частини тощо).

БІБЛІОГРАФІЧНИЙ СПИСОК

1. Смит Р. Э. Аутентификация: от паролей до открытых ключей. – М.: Изд. дом «Вильямс», 2002. – 432 с.
2. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. – К.: ООО «ТИД «ДС», 2001. – 688 с.
3. Хорошко В. А. Методы и средства защиты информации. – К.: Изд-во «Юниор», 2003. – 504 с.
4. Столингс В. Криптография и защита сетей. Принципы и практика; 2-е изд. – М.: Изд. дом «Вильямс», 2001. – 672 с.
5. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С; 2-е изд. – 2003.
6. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: Кудиц-образ, 2001. – 386 с.
7. Государственный стандарт Союза ССР. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. ГОСТ 28147-89 в действии от 01.09.90.
8. Аскеров Т. М. Защита информации и информационная безопасность: Учебн. пособ. / Под общей ред. К. И. Курбакова. – М.: Рос. экон. акад., 2001.
9. Анин Б. Защита компьютерной информации. – СПб.: БХВ-Петербург, 2000. – 384 с.

Надійшла до редколегії 30.03.2008.