УДК 004.9

О.М. ШИНКАРУК, О.М. ЯШИНА
Хмельницький національний університет

ВИКОРИСТАННЯ СМАРТ-КАРТ ДЛЯ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ІНФОРМАЦІЙНИХ СИСТЕМ

В даній статті обґрунтовується доцільність використання смарт-карт для ідентифікації користувачів під час доступу до інформаційних систем. Також показана можливість використання корпоративних ІТ-систем з інфраструктурою відкритих ключів PKI на базі алгоритму RSA.

Ключові слова: смарт-карта, інформаційні технології, інформаційні системи, PKI-система, метод RSA.

OLEG SHYNKARUK, OXANA YASHYNA
Khmelnitsky National University

USE OF SMART CARDS FOR IDENTIFICATION OF USERS OF INFORMATION SYSTEMS

Abstract – In this article the feasibility of using smart- cards for users identification during access to information systems has been analised. Also, the possibility of the use of corporate IT- systems with public key infrastructure PKI - based algorithm RSA has been discussed.

Keywords: smart card, information technology, information systems, PKI system, the RSA method.

Постановка задачі

Інформаційні технології застосовуються практично у всіх сферах економіки. Маленькі фірми та корпорації впроваджують у себе комп'ютерну техніку та створюють інформаційну інфраструктуру. Із збільшенням об'єму даних постає питання про їх безпечне зберігання, використання, обмін та ін. Однак найактуальнішим залишається завдання контролю доступу до цих даних. На ринку апаратно-програмного забезпечення найбільшим попитом, завдяки своїй доступності за рівнем цін, як правило користуються засоби, що потребують використання паролів для ідентифікації користувачів. З точки зору питань безпеки використання паролів втрачає свій сенс, оскільки часто трапляється, що працівники записують їх на папірцях, які лежать на робочих столах або приклеєні до моніторів. Це підвищує ймовірність крадіжки конфіденційної інформації, або створює умови для порушення доступу до даних. Крім того, важливо зауважити, що паролі, як єдиний механізм ідентифікації, цілком нормальні, якщо довжина пароля становить більше 15 символів і включає комбінацію цифр, літер у різних регістрах та літер із іншого алфавіту (не латинських), спеціальні символи. Ключові фрази є прикладами надійних паролів, які користувачам простіше запам'ятовувати. Це дозволяє бути впевненим в тому, що більшість атак не увінчаються успіхом саме завдяки доданій складності, якої надають «іноземні» символи [1].

Ще однією причиною, неефективності паролів як єдиного механізму ідентифікації, є невміння користувачами правильно підбирати і запам'ятовувати гарні, надійні паролі. До того ж паролі найчастіше не захищаються належним чином. Тому витік і слабкість паролів стає серйозною проблемою для ІТ-адміністраторів та відповідальних за інформаційну безпеку.

Однак, існують такі ІТ-рішення, які передбачають використання коротких, легких для запам'ятовування паролів, сприяючи підвищенню безпеки та зручності. На сьогоднішній день у економічно розвинених країнах найбільш розповсюдженим засобом ідентифікації користувачів є застосування смарт-карт, роль яких в корпоративній ІТ-безпеці останнім часом суттєво зросла. В Україні ж застосування смарт-технологій розвивається надзвичайно повільно, оскільки потребує значних капіталовкладень. Разом з тим застосування смарт-карт сприяє підвищенню рівня безпеки будь-якого підприємства чи організації, що в свою чергу не може не впливати на високу конкурентоздатність. **Метою статті** є визначення теоретичних аспектів застосування смарт-карт в торгівельних мережах для ідентифікації працівників.

Аналіз досліджень та публікацій

Методологічною основою нашого дослідження стали праці Фороузана Б. А., Шнайера Б. та інших. Деякими аспектами застосування смарт-технологій займались такі російські вчені як Шорін Д. В., Шкурко М.І., Борисенко О. В., Стасенко Л., Куліков А.Л. Загалом же в теперішній час виконується велика кількість різноманітних досліджень, присвячених застосуванню інформаційних технологій в розв'язанні економічних, соціальних та інших задач. Однак, наукових робіт, присвячених застосуванню смарт-технологій для ідентифікації користувачів інформаційних систем недостатньо, що і обумовило виявлення до цього питання підвищеного наукового та практичного інтересу.

Виклад основного матеріалу

Можливості, які зараз пропонують карткові технології, не обмежуються тільки доступом в приміщення (Physical Access). Крім цього, карти можна використовувати для організації логічного доступу до даних (Logical Access), електронного цифрового підпису, персональної ідентифікації, для зберігання захищених даних [2].

У загальному випадку, систему авторизації в корпоративних системах можна будувати на двох принципах: на основі «логін-пароль» і на основі цифрових сертифікатів. Смарт-карти можна застосовувати і в тому, і в іншому випадку.

На нашу думку в торгівельних мережах доцільним є застосування корпоративних ІТ-систем, що засновані на цифрових сертифікатах та інфраструктурі відкритих ключів (PKI). Зупинимося на них

детальніше.

Використання цифрових сертифікатів і криптографічних смарт-карт в корпоративних інформаційних системах дозволяє здійснювати так звану строгу двофакторну авторизацію. Авторизація називається двофакторною тому, що в процесі аутентифікації (підтвердження особистості користувача) одночасно використовується дві ознаки персони: предмет, яким володіє тільки даний користувач (персональна смарт-карта) та інформація, якою володіє тільки він (PIN-код для доступу до карти). Тільки при наявності та збігу цих ознак користувач може увійти в корпоративну інформаційну систему. Сувора двофакторна ідентифікація є, на нашу думку, найбезпечнішим способом авторизації в корпоративному середовищі. Пароля в таких системах просто не існує, відповідно, його неможливо вкрасти [2].

Застосування PKI-системи доцільно застосовувати на базі алгоритму RSA, оскільки такі системи підтримують всі ОС і додатки. До того ж, подібні системи досить просто впроваджувати і використовувати.

Алгоритм RSA ґрунтується на виразах зі степенями [5]. Відкритий текст шифрується блоками, кожен з яких містить двійкове значення, менше деякого заданого числа n. Це означає, що довжина блоку повинна бути менше або дорівнює $\log_2(n)$. На практиці довжина блоку вибирається рівною 2^k бітам, де $2^k < n \le 2^{k+1}$. Шифрування й дешифрування для блоку відкритого тексту M і блоку шифрованого тексту C можна представити у вигляді наступних формул:

$$C = M^e \bmod n, \quad M = C^d \bmod n = \left(M^e\right)^d \bmod n = M^{ed} \bmod n.$$

Як відправник, так і одержувач повинні знати значення n. Відправник знає значення e, і лише одержувачу відомо значення d. Таким чином, дана схема є алгоритмом шифрування з відкритим ключем $KU = \{e, n\}$ і особистим ключем $KR = \{d, n\}$. Щоб цей алгоритм міг використовуватися для шифрування з відкритим ключем, повинні бути виконані наступні вимоги.

1. Повинні існувати такі значення e, d і n, що $M^{ed} = M \bmod n$ для всіх $M < n$.
2. Повинні відносно легко обчислюватись M^e і C^d для всіх значень $M < n$.
3. Повинно бути практично неможливо визначити d за наявними e та n.

Знайдемо співвідношення виду:

$M^{ed} = M \bmod n$

Тут найкраще підійде наслідок теореми Ейлера: для таких будь-яких двох простих чисел p і q та будь-яких двох цілих чисел n і m, що $n = pq$ і $0 < m < n$, і довільного цілого числа k виконуються наступні співвідношення:

$$m^{k\phi(n)+1} = m^{k(p-1)(q-1)+1} \equiv m \bmod n,$$

де $\phi(n)$ є функцією Ейлера, значення якої дорівнює числу додатних цілих чисел, менших n і взаємно простих з n. У випадку простих p і q маємо $\phi(pq) = (p-1)(q-1)$.

Тому необхідне співвідношення виходить за умови:

$$ed = k\phi(n) + 1.$$

Що еквівалентно наступним співвідношенням:

$$ed \equiv 1 \bmod \phi(n), \quad d \equiv e^{-1} \bmod \phi(n).$$

Тобто e і d є взаємно зворотними по модулю $\phi(n)$. Зверніть увагу, що у відповідності з правилами арифметики в класах розрахунків, це може мати місце тільки тоді, коли d (а отже, і e) є взаємно простим з $\phi(n)$. У еквівалентному записі $\gcd(\phi(n), d) = 1$.

Тепер у нас є все, щоб представити схему RSA. Компонентами схеми це:

p і q – два простих числа	(секретні, вибираються),
$n = pq$	(відкрите, обчислюється),
Таке $\gcd(\phi(n), d) = 1, \quad 1 < e, \phi(n),$	(відкрите, вибирається),
$d \equiv e^{-1} \bmod \phi(n)$	(секретне, обчислюється).

Особистий ключ складається з $\{d, n\}$, а відкритий – з $\{e, n\}$. Припустимо, що користувач A опублікував свій відкритий ключ і тепер користувач B збирається переслати йому повідомлення M. Тоді користувач B обчислює $C = M^e \bmod n$, і пересилає C. отримавши цей шифрований текст, користувач A дешифрує його, обчислюючи $M = C^d \pmod n$.

Має сенс навести тут обґрунтування цього алгоритму. Ми вибрали e і d такі, що $d \equiv e^{-1} \bmod \phi(n)$.

Таким чином, $ed \equiv 1 \bmod \phi(n)$. Значить, ed має вигляд $k\phi(n) + 1$. Але за наслідком теореми Ейлера, для таких будь-яких двох простих чисел p і q і цілих чисел $n = pq$ і M, що $0 < M < n$, виконуються співвідношення:

$$M^{k\phi(n)+1} = M^{k(p-1)(q-1)+1} \equiv M \bmod n,$$

Тому $M^{ed} = M \bmod n$. Тепер ми отримали:

$$M = C^d \pmod n \text{ та } M = C^d \bmod n = \left(M^e\right)^d \bmod n = M^{ed} \bmod n.$$

Криптостійкість алгоритму RSA заснована на припущенні, що виключно важко визначити секретний ключ по відомому, оскільки для цього необхідно розв'язати задачу про існування дільників цілого числа. Дана задача є NP-повною. Відомі точні алгоритми для розв'язку даної задачі мають експоненціальну оцінку обчислювальної важкості, внаслідок чого неможливо отримати точні розв'язки для задач великої чи то навіть середньої розмірності. Більше того, саме питання існування ефективних алгоритмів розв'язку NP-повних задач дотепер є відкритим. В зв'язку з цим для чисел, що складаються з 200 цифр (а саме такі числа рекомендується використовувати), традиційні методи потребують виконання великої кількості числа операцій (близько 10^{23}).

Оцінка складності задачі дискретного логарифмування в залежності від довжини двійкового запису простого числа P (при правильному його виборі) приведені в таблиці 1.

Таблиця 1

Оцінка складності задачі дискретного логарифмування

Довжина P (в бітах)	**Складність визначення ключа x**	**Пам'ять, що використовується алгоритмом (в бітах)**	**Час розв'язку задачі на комп'ютері типу 10^9 оп/с**
128	$2*10^{12}$	$7*10^6$	Декілька хвилин
200	10^{16}	10^8	Декілька місяців
256	$9*10^{17}$	10^9	Декілька десятків років
512	$4*10^{24}$	$3*10^{12}$	Більше 100 років безперервної роботи
1024	10^{34}	10^{17}	
1500	10^{41}	$8*10^{20}$	
2000	$7*10^{47}$	10^{24}	
2200	10^{50}	10^{25}	

Всі асиметричні криптосистеми намагаються зламати шляхом прямого перебору ключів. Тому в асиметричних криптосистемах використовують довгі ключі. Для забезпечення еквівалентного рівня захисту ключ асиметричної криптосистеми повинен бути набагато довший ключа симетричної криптосистеми. Це одразу ж позначається на обчислювальних ресурсах, що потребуються для шифрування.

Для того щоб уникнути низької швидкості алгоритмів асиметричного шифрування, генерується тимчасовий симетричний ключ для кожного повідомлення і тільки він шифрується асиметричними алгоритмами.

Отже, в асиметричних криптосистемах важливо, щоб сеансові і асиметричні ключі були порівнянні відносно рівня безпеки, який вони забезпечують. Асиметричні відкриті ключі уразливі до атак прямим перебором якраз через те, що їх важко замінити. Якщо атакуючий дізнається секретний асиметричний ключ, то буде скомпрометовано не тільки поточна, але й всі наступні взаємодії між відправником і одержувачем. Тому алгоритм RSA є найбільш надійним для захисту інформації, а отже ідентифікації користувача і ми вважаємо за доцільне використання даного алгоритму під час використання смарт-карток в цілях збереження конфіденційності інформації.

Висновки

Як правило у торгівельних мережах працює велика кількість людей, які в силу своїх обов'язків повинні мати доступ до конфіденційної інформації. Однак, переважна більшість працівників не вміє підбирати і не може запам'ятовувати велику кількість паролів, які необхідні для доступу до інформаційної системи того чи іншого супермаркету.

Отже, рішенням проблеми, на нашу думку, є використання технологій, що дозволяють використовувати смарт-карти, які засновані на інфраструктурі відкритих ключів. В зв'язку із тим, що інформація, розміщена на смарт-картах шифрується за допомогою методів криптографії, забезпечується висока надійність та захищеність даних.

Література

1. http://www.winsecurity.ru/articles/multifactor-authentication-windows-part1.html
2. http://www.isbc.com/_about/news_/type_2/section_322/show_192/
3. Б. А. Фороузан. Математика криптографии и теория шифрования информация. Режим доступу – http://www.intuit.ru/department/security/mathcryptet/14/3.html.
4. Шнайер Б. Прикладная криптография. – М.: Триумф, 2003. – 815 с.
5. ftp://ftp.rsasecurity.com/pub/rsalabs/rsa_algorithm/rsa-oaep_spec.pdf

Надійшла 17.1.2013 р.
Статтю представляє: д.т.н. Шинкарук О.М.