УДК 004.052.42

МАРКОВСЬКИЙ О.П.,
ЗАХАРІУДАКІС ЛЕФТЕРИС,
ФЕДОТОВ М.Ф.

МЕТОД СТРОГОЇ ІДЕНТИФІКАЦІЇ ВІДДАЛЕНИХ АБОНЕНТІВ НА ОСНОВІ СТАНДАРТИЗОВАНИХ ШИФРОБЛОКІВ ТА ХЕШ-ПЕРЕТВОРЕНЬ

В статті пропонується метод підвищення ефективності ідентифікації абонентів багатокористувацьких систем за рахунок зниження ризику несанкціонованого доступу до її ресурсів та підвищення продуктивності ідентифікації.

З теоретичної точки зору найефективніші схеми ідентифікації мають за основу концепцію нульових знань. Відомі схеми, що реалізують цю концепцію використовують функціональні перетворення, основані на операціях модулярної арифметики, які реалізуються повільно. Для схем ідентифікації, що базуються на концепції нульових знань запропоновано новий метод, оснований на використанні стандартизованих шифроблоків та хеш-перетворень. Доведено, що використання запропонованої технології дозволяє прискорити ідентифікацію на 2-3 порядки.

This paper proposes a method for increasing of efficiency of of the multi-user system abonent identifications by impairing the risk of illegal access to system resources and by increasing of identification productivity.

From the theoretical point of view the most effectiveness schemes of abonent identification are based on conception of zero-knowledge. But known schemes which realized this conception utilized the function transformation based on modular arithmetic which calculate slowly. For zero-knowledge based identification performance increase the new method base on utilization of standard block ciphers and hash transformation has been proposed. It has been shown that utilization of proposed identification technology allowed to increase the identification rate by 2-3 orders.

Ключові слова: схеми ідентифікації, інтерактивна ідентифікація, ідентифікація на основі концепції нульових знань, шифроблоки, хеш-алгоритми.

Вступ

Інтегровані системи зберігання та обробки даних з колективним доступом відіграють зростаючу роль в глобальних процесах інформаційної інтеграції. Така інтеграція дозволяє підвищити ефективність комп'ютерної обробки даних за рахунок надання доступу до інформаційних, програмних та обчислювальних ресурсів широкому колу користувачів.

Розвиток інтегрованих систем обробки інформації значною мірою залежить від ефективності реалізації в них функцій захисту інформації та розподілення прав доступу. Ключова роль у вирішенні цієї проблеми належить засобам ідентифікації абонентів. Розширення використання багатокористувацьких систем пов'язане зі зростанням ризиків несанкціонованого доступу до їх інформаційних та обчислювальних ресурсів. Це зумовлено, з однієї сторони, ростом технічних можливостей для реалізації несанкціонованого доступу, а з іншого – збільшенням потенційних вигод з цього. Факторами, що підвищують ризик несанкціонованого доступу до ресурсів інтегрованих систем обробки інформації є розширення використання потенційно відкритих для стороннього впливу бездротових систем передачі даних комп'ютерних мереж, підвищення продуктивності обчислювальних засобів, що використовуються для несанкціонованого доступу, збільшення кількості віддалений користувачів, і, відповідно зменшення обчислювальних ресурсів, які використовуються для захисту від несанкціонованого доступу.

За цих умов необхідністю є адекватне вдосконалення всього арсеналу засобів, які виключають можливість несанкціонованого доступу до ресурсів інтегрованих систем, в тому числі методів та засобів ідентифікації їх віддалених абонентів.

Таким чином, задача підвищення ефективності ідентифікації абонентів багатокористувацьких систем є важливою і актуальною для сучасного етапу розвитку комп'ютерних та мережевих технологій.

Аналіз відомих технологій ідентифікації віддалених абонентів

Базовими критеріями ефективності будь-якої системи захисту є рівень захищеності, що досяга-

ється при її використанні та об'єм ресурсів, що застосовується для реалізації функцій захисту. Відповідно, в процесі розробки будь-якої системи захисту даних, в тому числі і засобів ідентифікації віддалених абонентів, потрібно досягати компромісу між рівнем захищеності та продуктивністю реалізації функцій захисту.

Складність проблеми визначається неможливістю побудови адекватної формальної моделі дій сторони, що намагається реалізувати незаконний доступ до ресурсів системи. В першому наближенні процедура ідентифікації має задовольняти таким вимогам [1]:

1) Організація зберігання ідентифікуючої інформації має бути такою, щоб одна її частина зберігалася у абонента, а друга – в системі і кожна з цих частин не була б самодостатньою для доступу до ресурсів системи.

2) Ідентифікаційна посилка абонента при кожному сеансі підключення до системи має змінюватися.

3) Об'єм секретної інформації, що зберігається в системі і використовується для ідентифікації має бути якомога меншим з тим, щоб надати можливість збереження такої інформації в спеціальній захищеній на апаратному рівні пам'яті.

Всі сучасні протоколи ідентифікації абонентів розділяють на два класи: з використанням паролів, що перевіряються системою шляхом порівняння ("слабка" ідентифікація) та на основі теоретичної концепції "нульових знань" ("строга" ідентифікація) [2].

В основі більшості протоколів ідентифікації віддалених абонентів лежить теоретична концепція "нульових знань". Сутність цієї концепції полягає в тому, що для доведення своєї автентичності абонент має неявним чином виявити знання певної інформації, якою система не володіє, але може перевірити її наявність у абонента.

При цьому в системі не зберігається ніякої секретної інформації, яка дозволяє відновити ідентифікаційні дані абонента, що пояснює походження назви концепції "нульових знань". Важливим є те, що при кожному зверненні до системи абонентом генерується нова ідентифікуюча інформація.

Таким чином, концепція нульових знань в теоретичному плані найбільш повною мірою відповідає сформульованим вище вимогам щодо системи ідентифікації абонентів. В сучасних умовах і у найближчій перспективі потрібний для практики рівень надійності ідентифікації може бути забезпечений лише методами, що спираються на концепцію "нульових знань".

Концепція "нульових знань" передбачає використання незворотних математичних перетворень. Це означає, що існує алгоритм перетворення в прямому напрямку, але принципово неможливим є аналітичне віднаходження алгоритму зворотного перетворення. В більшості існуючих схем ідентифікації на основі концепції "нульових знань" для реалізації такого перетворення використовуються аналітично нерозв'язувані задачі теорії чисел, зокрема відома задача дискретного логарифмування.

Найбільш відомими з схем ідентифікації цього класу є FFSIS (Feige Fiat Shamir Identification Scheme) [2], методи Шнора (Schnorr) та Гіллоу-Квіскватера (Guillou- Quisquater) [3]. Базовими обчислювальними операціями для FFSIS є $A^2 \cdot B \bmod m$, а для методів Шнора і Гіллоу-Квіскватера – $A^e \cdot B^v \bmod m$.

З викладеного слідує, що базовою обчислювальною операцією більшості схем строгої ідентифікації віддалених абонентів є модулярне експоненціювання над числами, довжина яких значно перевищує розрядність процесору. В умовах стійкої тенденції до зростання розрядності чисел, обчислювальна складність реалізації вказаного типу операцій збільшується експоненційно, випереджаючи темпи зростання продуктивності комп'ютерних систем.

Опубліковано [4] результати спроб використання при реалізації концепції "нульових знань" в якості незворотного булевих функціональних перетворень. Таке рішення дозволяє на порядки прискорити процедуру ідентифікації віддалених абонентів. Недоліками такого рішення є суттєве обмеження на кількість сеансів ідентифікації, складність процедури генерації незворотного та багатозначного булевого перетворення, значний об'єм пам'яті для зберігання в системі таблиць перетворень для кожного з абонентів. Суттєвим моментом є те, що не проведені об'ємні та всебічні дослідження рівня захищеності. Тому цей метод не дійшов до рівня практичного застосування в діючих протоколах ідентифікації.

Таким чином, основний недолік існуючих методів реалізації теоретично строгої ідентифікації на основі концепції "нульових знань" полягає в значній обчислювальній складності їх базових обчислювальних процедур. Ясно, що швидкість ідентифікації обмежується значною обчислювальною складністю цих операцій і, відповідно, виникає необхідність в її зменшенні.

Ціллю дослідження є зменшення обчислювальної складності процесу ідентифікації при забезпеченні високого рівня захищеності.

Метод ідентифікації на основі стандартизованих криптографічних примітивів

Для досягнення поставленої мети пропонується метод строгої ідентифікації віддалених абонентів, що реалізує теоретичну концепцію "нульових знань" з використнням стандартизованих шифроблоків та хеш-перетворень.

Стандартизований шифроблок (ШБ) являє сертифікований органами державної влади, алгоритм симетричного, тобто з використанням однакового ключа, шифрування-дешифрування блоку даних фіксованої довжини. До теперішнього часу найбільшого поширення набув шифроблок Rijndael [5], створений в рамках міжнародного проекту AES для заміни алгоритму шифрування першого покоління – DES. В ряді країн та окремих міжнародних корпораціях стандартизовано інші шифроблоки – фіналісти AES: MARS, SERPENT, RC-6 [6].

В структурному плані шифроблок в режимі шифрування можна розглядати як функціональний перетворювач φ, на входи якого подаються m-розрядний блок D даних та k–розрядний ключ K, а на виході формується m–розрядний блок C зашифрованих даних: $C = \varphi(D,K)$. Відповідно, в режимі дешифрування шифроблок реалізує зворотне перетворення φ^{-1}: на його входи подаються $\boldsymbol{m}$-розрядний блок C зашифрованих даних та k–розрядний ключ K, а на виході відновлюється m-розрядний блок даних $D=\varphi^{-1}(C,K)$. Для шифроблоку Rijndael регламентовано шифрування блоків, довжиною 128, 192 або 256 розрядів. В пропонованому методі використовується режим шифрування блоків довжиною 256 бітів (m = 256).

Стандартизований хеш-перетворювач (H) – сертифікований відповідними органами алгоритм незворотного перетворення інформаційного блоку довільної довжини в код хеш-сигнатури фіксованої розрядності h. Найбільш відомими є хеш-перетворювачі SHA-1 та RIPEMD-160 [1], що формують 160-бітову хеш-сигнатуру (h=160). Найважливішою якістю хеш-перетворювачів є їх незворотність – тобто практична неможливість віднаходження інформаційного блоку, хеш-сигнатура якого дорівнює заданій.

Для ефективної реалізації концепції нульових знань стосовно ідентифікації віддалених абонентів пропонується використання шифроблоку, довжина m блоку даних якого суттєво більша за розрядність h хеш-сигнатури. Зокрема, для практичного застосування методу пропонується використання шифроблоку з розрядністю блоку даних 256 (m=256) та хеш-перетворювачів з розрядністю хеш-сигнатури 160 (h=160). Різниця розрядностей блоку даних ШБ та хеш-сигнатури надалі позначається як $d=m-h$.

Головна перевага використання стандартизованих шифроблоків та хеш-перетворювачів полягає в тому, що їх криптостійкість надійно перевірена спеціальним тестуванням та в процесі практичного застосування.

Пропонований метод регламентує процедури ініціалізації та сеансової ідентифікації при кожному зверненні абоненту до системи.

Процедура ініціалізації включає два етапи:

1) Абонент випадковим чином формує d–розрядний двійковий код z, а також m–розрядний код R ідентифікатора абонента. Коди z та R в закритому режимі передаються в систему.

2) Абонент довільним чином обирає h-розрядний код q_n, після чого послідовно, з використанням стандартизованого хеш-перетворення H, обчислює n-1 h-розрядних кодів $q_{n-1}, q_{n-2},\ldots,q_2, q_1$ так, що кожен наступний з цих кодів являє собою хеш-сигнатуру попереднього, тобто, для кожного $i\in\{1,2,\ldots,n-1\}$: $q_i = H(q_{i+1})$. Сформовані таким чином коди зберігаються лише у абонента.

Процедура –то сеансу ідентифікації абонента полягає у виконанні наступної послідовності дій:

1) Абонент формує m-розрядний код сеансового ключа K_i як конкатенацію –розрядного коду q_i та d-озрядного коду z: $K_i = q_i|z$.

2) Абонент формується m-розрядний код U_i як результат зворотного шифрування коду R ключем K_i : $U_i = \varphi^{-1}(R,K_i)$. Пара кодів q_i та U_i утворюють (h+m)-бітовий i-тий сеансовий пароль: $P_i = < q_i, U_i >$.

3) Сеансовий пароль P_i передається системі.

4) Система розділяє отриманий сеансовий пароль на складові q_i та U_i.

5) Перевіряється правильність отриманого коду q_i шляхом перевірки того, що результат хеш-перетворення q_i збігається з кодом q_{i-1} попереднього сеансу ідентифікації, тобто перевіряється умова: $q_{i-1} = H(q_i)$. Якщо ця умова не виконується, то сеанс ідентифікації переривається.

6) Система конкатенацією отриманого коду q_i та секретного коду z формує сеансовий ключ K_i : $K_i = q_i|z$.

7) З використання сеансового ключа система виконує пряме шифрування m-розрядного коду U_i : $Y=\varphi(U_i, K_i)$.

8) Якщо отриманий в результаті шифрування код Y дорівнює коду доступу R абонента, тобто

$Y=R$, то ідентифікація абонента вважається успішною.

Таким чином, розроблений метод забезпечує ідентифікації віддалених абонентів з використанням паролей, що змінюються при кожному сеансі. При цьому система не здатна генерувати пароль, а може лише перевіряти його коректність. Перевірка виконується не через порівняння, а шляхом використанням незворотних перетворень. Відповідно, запропонований метод реалізує ідентифікацію, що цілком вкладається в рамки теоретичної концепції "нульових знань".

Оцінка ефективності

Порівняльна оцінка ефективності запропонованого методу ідентифікації віддалених абонентів може бути виконана за наступними критеріями:

- рівень захищеності від спроб отримати незаконний доступ до ресурсів системи як з боку сторонньої зловмисника, так і з боку осіб, що незаконно мають доступ до пам'яті системи;
- обчислювальна складність процедури ідентифікації системою;
- можливості апаратної реалізації ідентифікації системою, яка дозволяє збільшити рівень захищеності та прискорити процедуру ідентифікації;
-використання потенційно відкритих ліній обміну даними: чим менше використовуються такі лінії в процесі ідентифікації, тим менші можливостей незаконного доступу до ресурсів системи.

Запропонований метод реалізує концепцію строгої ідентифікації віддалених абонентів з використаннясм стандартизованих криптографічних примітивів.

Очевидно, що при кожному зверненні до системи абонент використовує інший пароль.

Сеансовий пароль i-го сеансу ідентифікації складається з двох складових q_i та U_i. В разі перехоплення послідовності паролей $P_1, P_2,\ldots,P_i$ стороннім зловмисником, його ціллю може бути відтвореня паролю P_{i+1} для наступного, $(i+1)$-го сеансу ідентифікації. Цей пароль складається з двох компонентів: h-розрядного коду q_{i+1} та m-розрядного коду U_{i+1}. Код q_{i+1} пов'язаний з кодом q_i попереднього сеансового пароля через співвідношення: $q_i = H(q_{i+1})$, тобто, для реконструкції q_{i+1} потрібно виконати зворотнє хеш-перетворення. Для стандартизованих хеш-перетворень єдиним методом реалізації зворотного перетворення є перебір. Іншими словами, для вирішення задачі реконструкції коду q_{i+1} по значенню попередньої компоненти q_i методом перебору, в середньому, потрібно виконати 2^{h-1} прорахунків хеш-перетвореня. Зокрема, для стандартизованого хеш-алгоритму SHA-1 потрібно перебрати, в середньому, 2^{159} варіантів.

Для реконструкції коду U_{i+1} сторонньому зловмиснику потрібно підібрати такий код, щоб виконувалася умова: $U_{i+1} = \varphi^{-1}(R,K_{i+1})$, при невідомих значеннях m-розрядних кодів R та K_{i+1}. Технологічно, підбір доцільно виконувати по відомому значенню U_i, з використаннім рівняння $\varphi(U_i, K_i) = \varphi(U_{i+1}, K_{i+1})$. Якщо до цього сторонній зловмисник теоретично зможе реконструювати код q_{i+1}, то йому потрібно підібрати m-розрядний код U_{i+1} для кожного з можливих значень d-розрядного коду z – закритої компоненти ключа K. Таким чином, об'єм перебору становить $2^{m+d} = 2^{2\cdot m-h}$. При використанні в якості шифроблоку алгоритму Rijndael, а в якості хеш-перетворення SHA-1, m=256 і h=160, тобто обєм перебору для реконструкції коду U_{i+1} може буди оцінений як 2^{352} реалізацій процедури шифрування за алгоритмом Rijndael, що виходить за рамки сучасних технічних можливостей.

Для імітації звернення абонента самою системою або реалізації незаконного доступу за наявності в розпорядженні зловмисника секретних кодів R та z, що зберігаються в системі, потрібно виконати реконструкцію коду q_{i+1} по значенню попереднього коду q_i. Як зазначалося вище, використання стандартизованого хеш-перетворює унеможливлює застосування для цього інших методів крім перебору. При цьому, в середньому, потрібно виконати 2^{h-1} прорахунків хеш-перетвореня, що для стандартизованого хеш-алгоритму SHA-1 становить 2^{159} реалізацій алгоритму і виходить за рамки практичної доцільності.

В перспективі, рівень захищеності запропонованого методу строгої ідентифікації, що реалізує концепцію "нульових знань" може бути підвищений за рахунок простого збільшення розрядності шифроблоку та хеш-сигнатури.

Найбільш важлива перевага запропонованого методу реалізації ідентифікації на основі концепції "нульових знань" в порівнянні з існуючими методами (схеми Fiat-Shamir, Schnorr) полягає в тому, що він забезпечує значне зменшення обчислювальної складності процедури ідентифікації. Більшість існуючих методів ідентифікації віддалених користувачів, що реалізують концепцію "нульових знань" мають за основу незворотні перетворення теорії чисел, базовою операцією яких є модулярне експоненціювання над числами великої розрядності – 2048 або 4096. За оцінками [4] обчислювальна складність операції експонен-

ціювання для розрядності 2048 на три порядки перевищує обчислювальну складність шифрування з використанням стандартизованого шиброблоку. Це означає, що обчислювальна складність запропонованого методу реалізації строгої ідентифікації на три порядки менша в порівнянні з відомими методами, що реалізують концепцію "нульових знань". На практиці це означає, що запропонований метод дозволяє на три порядки скоротити час ідентифікації абонента, що критично важливо для ефективності систем колективного доступу.

Значимою для практики перевагою запропонованого методу в порівнянні з відомими є також те, що шифроблоки та хеш-перетворення побудовані на логічних операціях, які просто та ефективно можуть бути реалізовані апаратними засобами, в тому числі ПЛІС [7]. Апаратна реалізація операцій модулярного експоненціювання над числами великої розрядності, що лежать в основі відомих методів строгої ідентифікації, суттєво більш складна і менш ефективна.

Орієнтація розробленого методу на використання стандартизованих шифроблоків та хеш-перетворень відкриває широкі можливості його реалізації з використанням мікросхем криптопроцесорів, що випускаються промисловістю провідних країн світу. Такі криптопроцесори на апаратному рівні реалізують стандартизовані шифроблоки та хеш-перетворення.

На відміну від відомих методів, для одного сеансу ідентифікації використовується лише одна пересилка пароля через потенційно відкриті лінії передачі даних.

Висновки

В результаті проведених досліджень запропоновано новий метод строгої, тобто такої, що має за основу концепцію "нульових знань", ідентифікації віддалених абонентів. Відмінність методу полягає в використанні стандартизований криптографічних примітивів: шифроблоків та хеш-перетворювачів.

Використання добре досліджених криптографічних примітивів, що пройшли перевіркою практичним застосуванням, забезпечує високий рівень надійності захисту від спроб порушення ідентифікації.

З іншого боку, обчислювальна складність шифроблоків та хеш-перетворювачів на три порядки менша за складність операції модулярного експоненціювання аналогічної розрядності. Це означає, що запропонований метод потребує на порядки менше операцій для своєї реалізації. Експериментальні дослідження показали, що реально швидкість програмної реалізації запропонованого методу строгої ідентифікації на 2-3 порядки вище в порівнянні з відомими методами FFSIS та Гіллоу-Квіскватера.

Список посилань

1. Schneier B. Applied Cryptography. Protocols. Algorithms and Source codes in C. -Ed.John Wiley, 1996 - 758 pp.
2. Feige U. Zero knowledge proofs of identity / Feige U.,Fiat A.,Shamir A.// Journal of Cryptology.- v.1.- №.2.- 1988, pp.77-94.
3. Pourand G. A realistic security analysis of identification schemes based on combinatorial problems // European Transactions on Telecommunications.- V.8,-№.5.- 1997,- pp.471-480.
4. Markovskyy O. Fast subscriber identification based on the zero knowledge principle for multimedia content distribution/ O. Markovskyy, N. Bardis, N. Doukas // International Journal of Multimedia Intelligence and Security 2010 - Vol. 1,- pp.78-82.
5. Зенин О.С. Стандарт криптографической защиты AES./ Зенин О.С., Иванов М.А. - М.:Из-во Кудиц-Образ.- 2002.- 174 с.
6. Elbirt A. An FPGA Implementation and Performance Evaluation of the AES Block Cipher Candidate Algorithm Finalists // Proceedings of The Third Advanced Encryption Standard Candidate Conference. NIST, Gaithersburg, MD,- 2000.- pp 13-27.
7. Марковский А.П. Аппаратная реализация алгоритма Rijndael на FPGA-структурах./ А.П. Марковский, В.А. Стефанская, С.В. Грищенко // Вісник Національного технічного університету України "КПІ" Інформатика, управління та обчислювальна техніка- № 38.- 2002,- С.24-33.