

МЕТОД СТРОГОЇ ІДЕНТИФІКАЦІЇ АБОНЕНТІВ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Марковський О. П., Захаріудакіс Лефтеріос., Федотов М.Ф.

Факультет інформатики та обчислювальної техніки

КПІ ім. Ігоря Сікорського, Україна

E-mail: markovskyy@i.ua

Method for strong users identification in telecommunication systems

The method for high speed remote users authentication has been proposed. Proposed method realized the zero-knowledge conception of cryptographically strong authentication. Developed method is based on using of standard hash transformation. The procedures for remote users registration and authentication cycle were developed in detail. It has been shown that utilization of proposed technology allowed to increase the identification rate by 2-3 orders.

Розвиток телекомунікаційних систем значною мірою залежить від ефективності реалізації в них функцій захисту інформації та розподілення прав доступу. Ключова роль в вирішенні цієї проблеми належить засобам ідентифікації абонентів. Виходячи з цього, вдосконалення таких засобів є важливим та актуальним для розвитку сучасних інформаційних та телекомунікаційних технологій.

Високий рівень ефективності ідентифікації віддалених абонентів досягається як результат певного компромісу між рівнем захищеності від несанкціонованого доступу та швидкістю ідентифікації.

Теоретично доведено [1], що найбільший рівень захищеності від спроб несанкціонованого доступу може бути досягнутий в рамках концепції "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.

Ідентифікація абонентів, що реалізують теоретичну концепцію "нульових знань" вважається [2] строгою.

Концепція "нульових знань" передбачає використання теоретично незворотних криптографічних перетворень. Це означає, що існує алгоритм перетворення в прямому напрямку, але принципово неможливим є аналітичне віднаходження алгоритму зворотного перетворення. В існуючих схемах ідентифікації на основі концепції нульових знань для реалізації такого перетворення використовуються аналітично нерозв'язувані задачі теорії чисел, зокрема відома задача дискретного логарифмування. На практиці найбільшого поширення набули методи FESIS [3], Guillou-Quisquater [4] та Schnorr [1].

Найбільш значимий для практики недолік існуючих схем строгої ідентифікації полягає в значній часовій складності обчислень, пов'язаних з реалізацією процедур ідентифікації. Це зумовлено тим, що в їх основі лежать мультиплікативні операції модулярної арифметики, що виконуються над числами, розрядність яких значно перевищує розрядність сучасних процесорів. Відповідно, висока складність обчислень значно сповільнює процес ідентифікації.

Авторами запропоновано метод реалізації строгої ідентифікації на іншій математичній основі - незворотних булевих функціях. Для реалізації таких перетворень пропонується використати стандартизовані хеш-перетворення. 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.

Суттєва перевага використання стандартизованих 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.

Метод передбачає таку послідовність дій при реєстрації :

- 1) Користувач довільно визначає кількість n циклів ідентифікації.
- 2) Випадковим чином генерує n -ий сеансовий пароль P_n .
- 3) Обчислює $n-1$ паролів, причому j -тий пароль P_j , $j=n-1, \dots, 0$ обчислюється як хеш-перетворення $H(x)$ від конкатенації попереднього паролю та номера сеансу: $P_j = H(P_{j+1} || j)$.

4) Пароль P_0 відсилається в систему, зашифрований її відкритим ключем.

Послідовність дій j -того сеансу ідентифікації має вигляд:

- 1) Користувач шифрує відкритим ключем системи j -тий сеансовий пароль P_j і відсилає його в систему.
- 2) Система виконує хеш-перетворення над конкатенацією отриманого паролю та номера сеансу: $\xi = H(P_j || j)$ і порівнює результату з попередньо отриманим паролем P_{j-1} : якщо $\xi = P_{j-1}$ то надається доступ.

Очевидно, що система, маючи в розпорядженні попередній пароль P_{j-1} не здатна сама генерувати наступний пароль P_j : ця задача еквівалентна злому стандартизованого хеш-алгоритму. Ці алгоритми ретельно тестовано, вони пройшли апробацію практикою, їх незворотність гарантована відповідними державними органами. Використання стандартизованого хеш-перетворює унеможливує застосування для цього інших методів крім перебору. При цьому, в середньому, потрібно виконати 2^{h-1} прорахунків хеш-перетворення, що

для стандартизованого хеш-алгоритму SHA-1 становить 2^{159} реалізацій алгоритму і виходить за рамки практичної доцільності.

Виходячи з цього, можна вважати, що задача підбору пароля як системою так і стороннім зловмисником потребує ресурсів, що виходять за рамки практичної доцільності.

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

Основною перевагою запропонованого методу в порівнянні з аналогами полягає в тому, що передбачені ним обчислення мають значно меншу складність. 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 [2] обчислювальна складність операції експоненціювання для розрядності 2048 на три порядки перевищує обчислювальну складність шифрування з використанням стандартизованого шифроблоку. Це означає, що обчислювальна складність запропонованого методу реалізації строгої ідентифікації на три порядки менша в порівнянні з відомими методами, що реалізують концепцію “нульових знань”. Проведені експерименти показали, що реально швидкість ідентифікації збільшується на 2-3 порядки.

Значимою для практики перевагою запропонованого методу в порівнянні з відомими є також те, що 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.

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

Література

1. Schneier B. Applied Cryptography. Protocols. Algorithms and Source codes in C. -Ed. John Wiley, 1996 - 758 pp.
2. 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.
3. Feige U. Zero knowledge proofs of identity / Feige U., Fiat A., Shamir A.// Journal of Cryptology.- v.1.- №.2.- 1988, pp.77-94.
4. Pourand G. A realistic security analysis of identification schemes based on combinatorial problems // European Transactions on Telecommunications.- V.8,-№.5.- 1997,- pp.471-480.