learning management systems:Sakai and Moodle, 2010. www.Monarchmedia.com. 8. Дьяченко А. В. Построение информационных систем непрерывного образования на основе интернет-технологий / А. В. Дьяченко, В. Г. Манжула, А. Э. Попов, И. Н. Семенихин, А. П. Толстобров. – Академия Естествознания, 2010. 9. Obringer, Lee Ann. How E-learning Works. 01 October 2001. HowStuffWorks.com. 10. Гайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV,2009. – 608 с.. 11. Охота Д. Б. Технології комп'ютерної безпеки [Текст] / Д. Б. Охота. – Рівне: МЕГУ, 2011. – 97 с. 12. Митні інформаційні технології: навчальний посібник / за ред. П. В. Пашка. – К.: Знання, 2011. – 391 с. 13. Руслан Коржик. Алгоритм шифрования MD5 // Компьютерная газета № 18, 2006 г. http://www.nestor.minsk.by/kg/. 14. Організація баз даних та знань: підручник / В. В. Пасічник, В. А. Резніченко. – К.: Видавнича група BHV, 2006. – 384 с.

УДК 681.3

А. О. Ігнатович
Національний університет "Львівська політехніка",
кафедра електронних обчислювальних машин

МЕТОД АДАПТИВНОЇ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ У КОМП'ЮТЕРНИХ МЕРЕЖАХ НА ОСНОВІ БІОМЕТРИЧНИХ ДАНИХ

За результатами аналізу особливостей захисту інформації в комп'ютерних мережах обґрунтована потреба застосування біометричних даних у сервісах аутентифікації користувачів. Запропоновано метод адаптивної автентифікації користувачів у ступеневій системі захисту інформації у комп'ютерній мережі на основі біометричних даних – відбитків пальців.

Ключові слова: захист інформації, аутентифікація, комп'ютерна мережа, біометричні дані, відбитки пальців.

BIOMETRIC DATA BASED METHOD OF ADAPTIVE USER AUTHENTICATION IN COMPUTER NETWORKS

According to the analysis of peculiarities of data protection in computer networks the necessity of usage of biometric data in user authentication services is founded. Adaptive method of user authentication in multilevel data protection system of computer network based on biometric data of fingerprints is introduced.

Key words: data protection, authentication, computer network, biometric data, fingerprints.

Вступ

Проблема захисту інформації від суб'єктів, які не мають на це права, має багатолітню історію. Особливо актуальною стала ця проблема тепер, під час масового застосування комп'ютерних технологій. Велика кількість вчених та дослідників працюють над ефективним розв'язанням цієї багатогранної проблеми. За результатами цих досліджень сформувалися такі напрями наукових досліджень, як криптографія та захист інформації. Багато розроблених методів,

алгоритмів, засобів захисту інформації, передусім в комп'ютерних мережах, мають переваги та недоліки. Відповідно, дослідження щодо розширення функціональних можливостей та підвищення ефективності захисту інформації в комп'ютерних мережах є актуальними.

Огляд літературних джерел

Серед багатьох літературних джерел, що стосуються криптографії та захисту мереж, виділимо наважливіші. В монографії [1] розглянуто основні поняття сучасної криптографії, в монографії [2] – загальні принципи криптографії та особливості захисту комп'ютерних мереж. До основних функцій, які мають виконувати засоби захисту інформації, зараховують конфіденційність, аутентифікацію, цілісність, доступність, керування доступом. Конфінденційність – це гарантія можливості користування інформацією наперед визначеним суб'єктам та гарантія неможливості доступу до цієї інформації зловмисникам. Конфінденційність має забезпечити захист сховищ даних, передавання даних через канали зв'язку, неможливість виявити джерела та приймача повідомлення, частоту повідомлень, їх розміри. Аутентифікація – це гарантія надійної ідентифікації джерела повідомлення та встановлення факту, що джерело та приймач повідомлення не є підробними. Крім того, в процесі обміну даними засоби аутентифікації повинні не допускати, щоб на зміст інформаційного потоку мав можливість впливати зловмисник. Цілісність – це гарантія того, що прийняті повідомлення точно відповідають переданим. Доступність – це забезпечення можливості авторизованим суб'єктам використовувати інформацію, що зберігається на комп'ютерах мережі. Керування доступом передбачає можливість контролю за користуванням інформаційними ресурсами або системою, що володіє цими ресурсами, або системою, якій надано ці ресурси у користування. Крім розглянутих основних функцій, на засоби захисту інформації можуть покладатися додаткові функції, зумовлені особливостями використання ресурсів мережі.

Вважається, що аутентифікація та пов'язані з нею питання використання цифрових підписів є найбільш досліджуваною та спірною частиною теорії та практики захисту комп'ютерних мереж [2]. Останнім часом активізувалися дослідження щодо застосування біометричних даних для вирішення проблеми захисту інформації в комп'ютерних мережах. Біометричні дані – унікальна, вимірна характеристика людини, що може застосовуватись для ефективної ідентифікації або верифікації за прийнятний час із використанням обчислювальних можливостей комп'ютерів. В роботі [3] запропонована модель взаємодії користувача із системою криптографічного захисту на основі біометричних даних. В монографії [4] розглянуто основні принципи біометричної аутентифікації та криптографічного захисту. В роботах [5–8] запропоновано використання біометричних даних для захисту інформації в ГРІД-системах. Однак наведені результати досліджень не вичерпують можливості застосування біометричних даних для вирішення проблеми захисту інформації в комп'ютерних мережах.

Завдання дослідження

Дослідити додаткові можливості застосування біометричних даних для забезпечення функції автентифікації у засобах захисту інформації комп'ютерних мереж.

Основні результати дослідження

В засобах автентифікації повідомлень та цифрових підписів можна виділити два функціональні рівні. На нижньому рівні повинна виконуватися деяка функція, що генерує аутентифікатор – посвідчення, що використовується для аутентифікації повідомлення. Результат виконання цієї функції нижнього рівня потім використовуються як примітив у протоколі аутентифікації вищого рівня, що надає приймачеві повідомлення можливість перевірити правильність повідомлення [2]. Процес генерування аутентифікатора може використовувати функції трьох класів: а) шифрування повідомлень; б) код автентичності повідомлення (Message Authentication Code – MAC); в) хешування – автентифікатор використовує значення, що формується деякою відкритою функцією, яке для повідомлення довільної довжини має фіксовану довжину.

Основними біометричними даними людини вважають відбитки пальців, будову сітківки очей, тембр голосу. Найпоширенішими у системах захисту та обмеження доступу вважаються відбитки

пальців [3, 4]. Вони дають змогу отримати інформацію про всі десять пальців рук кожного користувача і застосовувати для задач захисту мереж малюнок будь-якого з них. Використання біометричних даних в окремих випадках ефективніше порівняно з такими засобами, як паролі, PIN-коди, смарт-карти та інші технічні пристрої, оскільки біометрія дає змогу ідентифікувати людину, а не пристрій. В основу біометричної ідентифікації за відбитком пальця покладена унікальність для кожної людини малюнка папілярних узорів на пальцях. Зображення відбитка пальця, отримане за допомогою спеціального сканера, перетвориться на цифровий код (згортку) і обробляється комп'ютером за необхідними алгоритмами, зокрема порівнюється з раніше введеним шаблоном (еталоном) або набором шаблонів (у разі ідентифікації). Серійно випускають недорогі спеціальні сканери, що забезпечують ефективне зчитування відбитків пальців. Обчислювальні потужності сучасних комп'ютерів забезпечують обробку біометричних даних за складними алгоритмами за прийнятний для засобів захисту інформації час. Відповідно можна застосувати адаптивний метод аутентифікації користувача в комп'ютерній мережі. В сервісах аутентифікації важливим етапом є формування та використання зашифрованих індивідуальних ключів. Виконання цього етапу доцільно адаптувати до особливостей захисту інформації кожним користувачем мережі. Біометрична інформація про всі десять пальців рук кожного користувача надає можливість адаптувати реалізацію індивідуальних ключів до конкретних особливостей мережі. Параметричну адаптацію можна реалізувати використанням різних ключів, рознесених у часі за наперед визначеним розкладом, узгодженим між учасниками повідомлень. Використання різних ключів можна реалізувати за формулою:

$$A = (C1 * C2) \bmod a,$$

де *A* – номер індивідуального ключа із урахуванням відбитка пальця; *C1*, *C2* – ідентифікаційні числа; a – довільне число від 2 до 10. Ідентифікаційні числа C1, C2 можуть бути як випадковими, так і мати наперед визначене інформаційне навантаження. Найбільші функціональні можливості, якщо *a = 10*.

Реалізуючи адаптивний метод, доцільно використати модель та алгоритм взаємодії між користувачем та засобами криптографічного захисту [3, 7].

Загальні особливості моделі та алгоритму взаємодії між користувачем та засобами криптографічного захисту такі. Спочатку необхідно створити деякий криптографічний примітив, який зв'яже закриті (приватні) ключі користувача мережі з частинками відбитків пальців. Необхідно створити певний масив даних, які в певний спосіб блокують наші закриті ключі. Такий процес формування необхідного масиву даних відбувається під час реєстрації нового користувача, або коли існуючий користувач змінює ключ.

Запропонований алгоритм створює з N вхідних наборів частинок біометричних даних, блокуючи множину W із S +1 елементів у полі F закритого ключа шифрування M із k елементів у полі F, який записується у вигляді коефіцієнтів полінома $f(x)$ степеня $k-1$ у полі $F: f(x) = m_1 + m_2 x + ... + m_k x^{k-1}$ [7].

Для досягнення криптографічної стійкості алгоритму блокування необхідно додати до множини W ряд фіксованих частинок. Після такого додавання загальна кількість частинок дорівнюватиме r. Доведено, що r визначається як мінімальне можливе значення відстані L між частинками, яка строго більша, ніж $2\sigma_s$, де σ_s – середня порогова відстань, що залежить від технології отримання наборів частинок (технічні характеристики сканера, властивості методу обробки зображень тощо). Тобто чим менша L, тим більше значення r, та як наслідок, стійкіший криптографічний захист. Але експериментально встановлено, що зі збільшенням r збільшується ймовірність помилкового декодування або помилкового відсотка браку (FRR) [7]. З іншого боку, кількість і розташування фіктивних часток обмежені дійсним розміщенням особистих часток і стандартним відхиленням розміщенням цих частинок.

Доцільно визначити параметри алгоритму k, s, r. Коефіцієнти полінома $f(x)$ є елементами скінченного (обмеженого) поля $F = GF(n)$. Оскільки у пропонованому підході ми розв'язуємо

поліноміальну інтерполяційну задачу, то для схеми "нечітке сховище" ефективними є коди корекції помилок Ріда–Соломона (RSC). Для виконання алгоритму декодування коду слід використовувати поле з $n = g^z$ елементів, де g – просте число. Одночасно поле для алгоритму блокування являє собою набір пікселів зображення відбитка пальця. Сучасні сканери мають формат кадра не менше ніж 256 x 256 пікселів. Ефективна область сканування – це ділянка, на яку припадає основна частина зображення (≈ 98 %). Цей висновок дає змогу визначити просте число. Найближче значення до цих цифр має область площею 251 x 251 пікселів, яка формує поле $\mathrm{F} = \mathrm{GF}(251^2)$.

Довжина полінома, значення k, визначається довжиною закритого (приватного) ключа блокування. Кожен з елементів поля $\mathrm{GF}(251^2)$ має розмірність 16 бітів. Отже, 256-бітному закритому ключу відповідає довжина у 16 поліноміальних коефіцієнтів, або поліном 15-го степеня.

Для перетворення координат розміщення реальних і фіктивних (вигаданих) часток у полях елементів доцільно використовувати 16-розрядні цілі числа x_i, в яких молодші 8 бітів відповідають ординатам, а старші біти – абсцисам.

Вихідним результатом алгоритму блокування є набір кортежів B_P, який складається з s пар $\{w_i, f(x_i)\}$ і $r - s$ пар фіктивних точок $\{\alpha_i, \beta_i\}$ з F, які задовольняють умову $f(\alpha_i) \neq \beta_i$. Щоб відкрити систему, яка використовує B_P, зловмисник повинен виявити цей набір точок, що належать многочленові $f(x)$, тобто виявити закритий (приватний) ключ. Очевидно, що чим більше значення r, тим більшою буде кількість подібних до $f(x)$ недостовірних (фальшивих) многочленів, а, отже, буде і вища стійкість системи до злому. Для зареєстрованого (легального) користувача системи потрібно і достатньо представити принаймні $\tau \geq k$ дійсних точок, щоб успішно інтерполювати неявний поліном. Для алгоритму розблокування формується набір $W' \subset F$, в якому міститься тільки частина елементів множини W. Отже, різниця двох наборів частинок дорівнює $\#(W - W') = t$.

Щоб розблокувати ключ шифрування з B_P, користувач надає набір особистих частинок, утворюючи відкриваючу множину $W' = \{w_1', ..., w_r'\}$. Розблокування відбувається, коли користувач запитує у системи закрите ключове питання.

Через W' і B_P видобувається множина B_P' найближчих (із граничною відстанню σ_s) частинок з потужністю r, де $r \approx s$ для зареєстрованого (легального) користувача, та $r >> s$ – для незареєстрованого (нелегального) користувача. Найменше допустиме значення $\tau = \dfrac{s+k}{2}$ [7].

Використовуючи аналогічний метод, можна оцінити ефективність алгоритму розблокування залежно від кількості дійсних частинок.

Необхідно враховувати, що чим більше значення r, тим складніший процес розблокування для незареєстрованого (нелегального) користувача, водночас це також збільшує складність для зареєстрованого користувача. k є ще одним важливим параметром, який впливає на ефективність алгоритму. Дослідження показали складність атаки як функцію з аргументами k і кількість реальних (дійсних) точок. Залежності показують зменшення стійкості і збільшення помилкового відсотка браку (FRR) одночасно зі збільшенням можливості корекції біометричних невизначеностей.

Засоби автентифікації користувачів на основі біометричних даних доцільно використовувати як спеціальне "біометричне" розширення сертифікатів X.509.v3. Такі засоби ефективні для грід-систем та розподілених комп'ютерних мереж. У разі делегування прав користувачам у грід-середовищі виконуватимуться такі дії: після взаємоідентифікації користувача і служби, що працюватиме від імені користувача, служба створює нову пару ключів і надсилає відкритий ключ користувачеві для підписання; користувач реєструється закритим (приватним) ключем, аналогічним до ключа

у центрі сертифікації. Отримані проксі-сертифікат і новозгенерований тимчасовий ключ можуть бути використані для служб автентифікації авторизованого користувача у всіх вузлах комп’ютерної системи чи мережі.

Висновки

Проведений аналіз особливостей захисту інформації в комп'ютерних мережах показав доцільність застосування біометричних даних у сервісах автентифікації користувачів. Запропоновано метод адаптивної автентифікації користувачів у комп'ютерних мережах на основі відбитків пальців. Обгрунтовано доцільність введення алгоритмів застосування біометричних даних у відповідні стандарти із сертифікації індивідуальних паролів у системах захисту інформації.

1. Ємець В. Сучасна криптографія: основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів: БАК. – 2003. – 144 с. 2.Столлингс В. Криптография и защита сетей: принципы и практика: пер. с англ. 2-е изд. – М.: Вильямс, 2001. – 672 с. 3. Варецький Я. Модель взаємодії користувача із системою криптографічного захисту / Я. Варецький, А. Ігнатович // Зб. наук. пр.: Вісник Львівського державного університету безпеки життєдіяльності МНС України. – 2007. – №1. – С. 143–149. 4. Русин Б. Біометрична аутентифікація та криптографічний захист: монографія / НАН України, Фіз.-мех. ін.-т ім. Г. В. Карпенка. – Львів: Коло, 2007. – 287 с. 5. Варецький Я. Особливості застосування біометричної інформації в ланках аутентифікації ГРІД-середовища / Варецький Я., Ігнатович А. Проблеми корозійно-механічного руйнування, інженерія поверхні, діагностичні системи // Матеріали відкритої науково-технічної конференції молодих науковців і. спеціалістів Фізико-механічного інституту ім.. Г. В. Карпенка НАН України. – Львів. – 2009. – С. 287–289. 6. Varectskyy J., Rusyn B., Ignatovych A.: Biometric Data Embedding in X.509 Certificates for Grid Systems // Informatyka w dobie XXI wieku. Technologie informatyczne w nauke, technice i educacji, pod red. A. Jastriebowa. – 2009. – P.145–148. 7. Varectskyy J., Rusyn B., A. Molga and Ignatovych A. A New Method of Fingerprint Key Protection of Grid Credential. // Advances in Intelligent and Soft Computing. Springer – Verlag Berlin Heidelberg. – 2010. – P. 99–104. 8. Standard ECMA-219. Authentication and Privilege Attribute Securite Applic Related Key Distribution Functions // ECMA. – 1994. – Parts 1, 2, 3. – P.176.