DOI 10.31891/2307-5732-2019-275-4-195-198
УДК 004.891

О.В. ОГНЄВИЙ, О.І. АКАТОВ, В.П. НЕЗДОРОВІН
Хмельницький національний університет

МЕТОД КОНТРОЛЮ ЦІЛІСНОСТІ КОНФІДЕНЦІЙНИХ ДАНИХ НА ОСНОВІ ФУНКЦІЙ ХЕШУВАННЯ

Відмови апаратного і програмного забезпечення, несанкціонований доступ, хакерські атаки – це ті загрози, для захисту від яких прикладаються великі зусилля. Для виключення можливості безслідної зміни заднім числом або видалення зареєстрованої інформації, в роботі запропоновано і досліджено метод для контролю цілісності зареєстрованої інформації. Під контролем цілісності інформації розуміється контроль тотожності символьного рядка перевірочної інформації відповідному рядку зареєстрованої раніше інформації. Мета полягає в розвитку алгоритмів, що забезпечують простий, загальнодоступний і надійний контроль цілісності конфіденційної інформації. Для досягнення зазначеної мети поставлено такі завдання: розвиток методу об'єктивного контролю цілісності інформації, заснованого на формуванні структури об'єднаних хешів, і розробка алгоритмів контролю і відновлення цієї структури з використанням розподіленого зберігання; розробка та дослідження алгоритмів хешування для оптимізації контролю цілісності інформації при зберіганні і передачі. Суть методу полягає в забезпеченні простоти, доступності, надійності та прозорості контролю цілісності даних в організаціях безпаперового документообігу, в забезпеченні авторських та інших прав, для програмного забезпечення нових видів банківського обслуговування, а також для вирішення інших завдань.

Ключові слова: інформаційні технології, захист інформації, конфіденційність інформації, контроль цілісності даних.

O.V. OHNIEVYI, O.I. AKATOV, V.P. NEZDOROVIN
Khmelnytskyi National University

METHOD FOR CONTROL INTEGRITY OF CONFIDENTIAL DATA BASED ON HASH FUNCTIONS

Failure of hardware and software, unauthorized access, hacker attacks are threats for the defence of which put great effort. In order to exclude the possibility of a consequent change or the delete of the registered information, in this work is proposed and investigated a method to control the integrity of the registered information. Control of the integrity of information is the control of the identity of the character string of the checking information to the corresponding line of previously registered information. The purpose is to develop algorithms that provide a simple, public and reliable control of the integrity of confidential information. To achieve this goal the following tasks are set: development of the method of objective control of the integrity of information based on the formation of the structure of mixed hashes, and the development of algorithms for control and restoration of this structure using distributed storage; development and research of hashing algorithms for optimization of information integrity control during storage and transmission. The essence of the method is to ensure the simplicity, accessibility, reliability and transparency of controlling the integrity of the data in the organizations of paperless circulation of documents, in providing copyright and other rights, software for new types of banking services, as well as for other tasks.

Key words: information of technologies, security information, confidentiality of information, data integrity control.

Вступ

В умовах глибокого проникнення інформаційних технологій в усі сфери життєдіяльності людини надійність ідентифікації інформації та контроль її цілісності стають важливою проблемою, причому як науково-технічною, так і соціальною. Науково-технічна проблема включає в себе створення математичних підходів, алгоритмів, програмного та апаратного забезпечення для вирішення цієї проблеми. Соціальний аспект проблеми пов'язаний з необхідністю створення загальнодоступної, зручної і захищеної системи надійної ідентифікації даних, адекватного ступеня розвитку інформаційних технологій.

Надійність ідентифікації інформації визначає в значній мірі і захищеність інформації, яка є «першорядним фактором, що впливає на політичну і економічну складові національної безпеки».

За існуючими оцінками більше 90% компаній стикалися з внутрішніми вторгненнями, більше половини стикаються з ними постійно, а втрати компаній тільки в США приблизно до 1 трлн дол. США. Велика частина втрат пов'язана з діями співробітників самих цих компаній, так як існуючі методи контролю цілісності даних контролюються самими власниками БД. Причинами свідомого корпоративного або особистого порушення цілісності інформації – видалення, спотворення, підміни – можуть бути помста, користь, страх, примус, вандалізм, цікавість, марнославство, самоствердження, кар'єрні ідеї, конкуренція, диверсія, саботаж та інші. Про частини порушень цілісності даних власник не повідомляє, приховуючи їх з різних причин: через відповідальність юридичну і комерційну, турботу про репутацію, вигоду від зробленого порушення, безвідповідальність, низьку кваліфікацію і т.п. Про приховування власниками БД відомих їм інсайдерських порушень цілісності даних повідомляє 78% респондентів цільового опитування і близько 90% відсотків опитаних при цьому вважають, що такий стан пов'язаний з нестачею ресурсів для управління. З останнього випливає висновок, що використання існуючих систем контролю цілісності даних вимагає занадто великих зусиль для забезпечення цього контролю і допускає приховування порушень цілісності даних.

Частину порушень цілісності інформації не знає найчастіше і сам власник БД. У деяких випадках власник БД не може виявити порушень цілісності інформації, що зберігається в БД інформації і при бажанні, особливо у випадках, наприклад, цілеспрямованого спотворення, введеного особами, які мають

санкціонований доступ до БД.

Постановка задачі

Метод контролю цілісності інформації заснований на використанні інформації, що міститься в контрольному ядрі. При цьому завдання забезпечення збереження цієї інформації вирішується, зокрема, широким поширенням реплікації контрольного ядра і описаними в роботі можливостями для перевірки його цілісності.

Усі існуючі методи, які призначені для контролю цілісності інформації, неефективні при цілеспрямованих інформаційних атаках, в тому числі за участю самих власників баз даних.

Для виключення можливості знищення контрольного ядра або спотворення його змісту будь-якими особами метод об'єднаних хешів передбачає поширення контрольного ядра в інформаційній мережі і пропонує алгоритми експлуатації таких розподілених відомостей про контрольне ядро, засновані на доведених властивостях контрольних ядер і їх фрагментів.

Основна частина

Від властивостей хеш-функцій залежать надійність даного методу, швидкість обчислень і ефективність використання обчислювальних ресурсів.

Особливості застосування хеш-функцій для цілей формування контрольних ядер об'єднані з необхідністю хешування конкатенації рядків; з необхідністю хешування відкритих рядків, тобто рядків з можливим продовженням; з властивостями хеш-функцій.

Нижче показаний загальний принцип хешування інформації за алгоритмом послідовного хешування.

Структура процедури хешування інформації включає такі етапи:

Етап 1. Формування контрольного ядра (вхідна інформація).

Етап 2. Операція хешування за допомогою алгоритму.

Алгоритм послідовного хешування з використанням логічних операцій використовує послідовне застосування обраних спеціальним чином логічних операцій до пар значень розрядів, один з яких є розрядом рядка хеша, а інший – розрядом хешуючого рядка.

У даному варіанті алгоритму номер кожної наступної логічної операції визначається за формулою:

$$I_k = (I_{k-1} + 1 + t_k)^{\mathrm{mod}\,8}, \quad (1)$$

де I_k – номер наступної логічної операції, I_{k-1} – сума попереднього номера логічної операції, t_k – значення поточного оброблюваного розряду хешуючого рядка.

Недоліком такого підбору номера логічної операції є легка прогнозованість цього номера для кожного розряду хешуючого і пов'язаного рядка. Іншим його недоліком є необхідність зберігання номера попередньої застосованої логічної операції, що незручно при розпаралелюванні процесу обчислення хеша за даним алгоритмом і перешкоджає застосуванню для прискореного обчислення хеша рядка, для якого відомий хеш його початкової частини.

Для виключення цих недоліків запропоновано наступний порядок вибору номера чергової застосовуваної логічної операції:

$$I_i = (|\, \underline{h}_i \underline{h}_{i+1} \underline{h}_{i+2} \,| + i + \underline{t}_k)^{\mathrm{mod}\,8}, \quad (2)$$

де i – номер розряду оброблюваного рядка хеша, $\underline{h}_i$ – значення i-го розряду рядка хеша, $\underline{t}_k$ – значення оброблюваного розряду хешуючого рядка, а $|\underline{h}_i\ \underline{h}_{i+1}\ \underline{h}_{i+2}|$ – число, представлене трьома значеннями розрядів хеша.

При використанні цього алгоритму розпаралелювання не повинно зменшувати інтервали між одночасно оброблюваними розрядами рядка хеша менш ніж до трьох розрядів.

Для прискорення алгоритму формула може бути простішою:

$$I_i = (|\, h_1 h_2 h_3 \,| + i + |\, h_i \,|)^{\mathrm{mod}\,8} \quad (3)$$

Хешування за допомогою псевдовипадкового рядка полягає в наступному: чергове наближення бінарного рядка хеша H_{i+1} довжиною в до розрядів $(h_1\text{-}h_k)$ отримують з попереднього наближення H_i складанням по модулю 2^k або побітовим складанням (XOR) з рядком довжиною в k розрядів.

$$H_1 = (H_0 + d_1) \bmod 2^k = (d_0 + d_1)^{\mathrm{mod}\,8^k}, \quad (4)$$

де k – число розрядів хеша (довжина хеша), d_i – відрізки псевдовипадкового бінарного рядка по k розрядів, які обираються за заданим алгоритмом, H_i – i-е наближення хеша, k – число розрядів хеша (довжина хеша).

Для варіанту з використанням побітового складання (XOR):

$$H_1 = H0 \ \vee\ \mathrm{d}_1 = d_0 \vee d_1 \quad (5)$$

Аналогічно, враховуючи, що

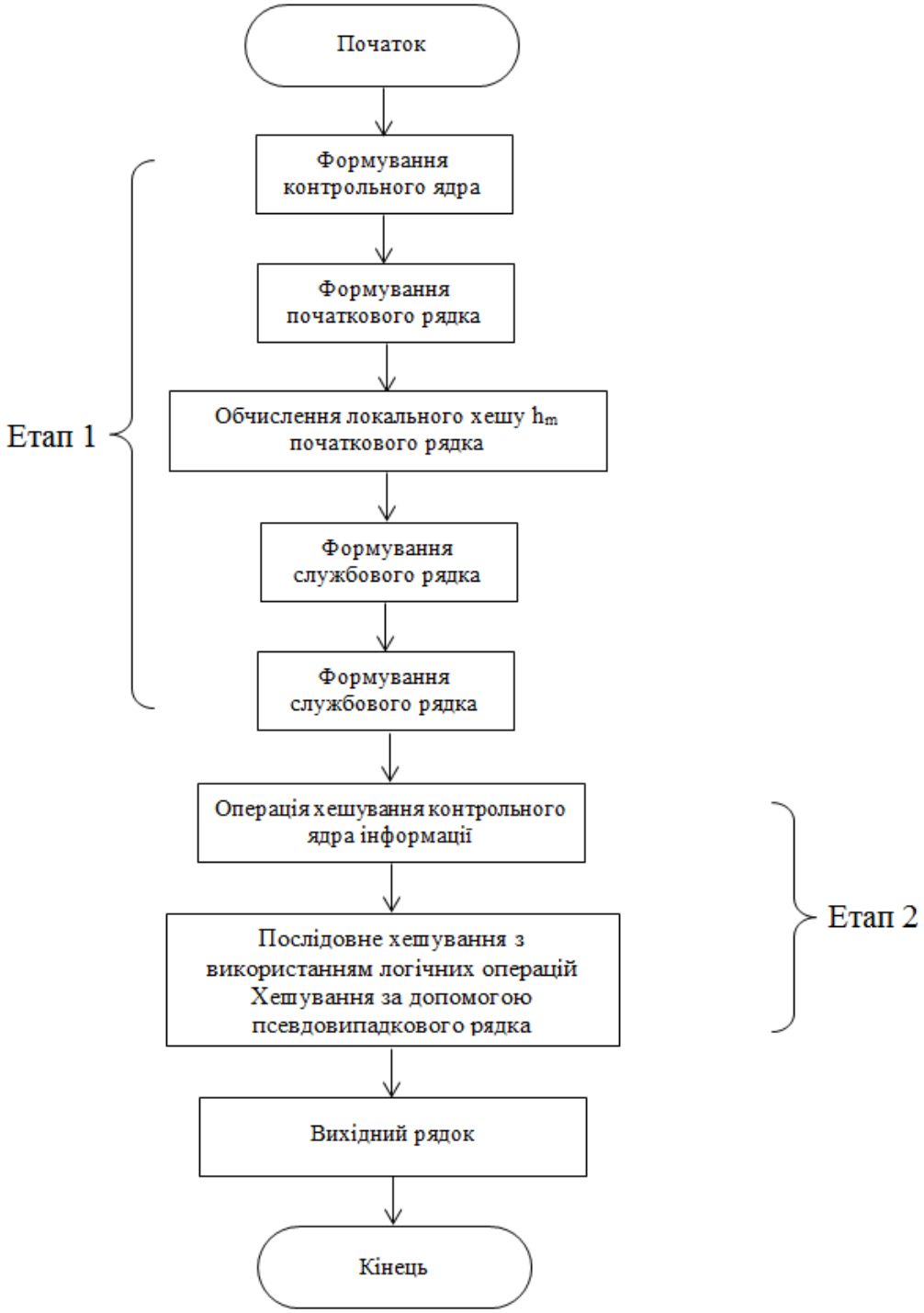

Рис. 1. Блок-схема загального принципу хешування інформації

$$N_i = | m | + | p_1 | + | p_2 | + ... + | p_i |, \quad (6)$$

де $|m|$ – модуль бінарного рядка, *pi* – блоки по *r* розрядів, на які розбитий рядок *m*.

Отримуємо для *i* наближення:

$$H_1 = (H_i - 1 + d_i)^{\bmod 2^k} = (d_0 + d_1 + ... + d_i - 1 + d_i)^{\bmod 2^k} \quad (7)$$

або при використанні побітового складання (для варіанту з XOR):

$$H_1 = H_{i-1} \vee d_i = d_0 \vee d_1 \vee ... \vee d_i - 1 \vee d_i \quad (8)$$

Останній варіант, звичайно, швидше, тому що XOR швидше складається.

Висновки

Представлений новий метод, який використовує алгоритми хешування з використанням логічних

операцій і з використанням псевдовипадкового рядка, має широкий потенціал застосування в різних областях діяльності: державної, громадської, фінансової, юридичної, виробничої, інформаційної, технічної.

Даний метод контролю цілісності даних дозволяє використовувати його для контролю цілісності:

інформації, що зберігається як в локальних, так і в глобальних БД;

інформації, що не поміщена в БД, в т.ч. не поміщена в базу даних, в якій зберігається контрольне ядро або його частина;

інформації, про яку при реєстрації відомий тільки її хеш;

інформації, що не зберігається взагалі (наприклад, інформації, яка була видалена після реєстрації);

будь-якої інформації вираженої в символьній формі.

Література

1. Петров А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. – Москва, 2013. – С. 448–452.

2. Лёвин В.Ю. О повышении криптостойкости однонаправленных хеш-функций. Фундаментальная и прикладная математика / Лёвин В.Ю. – Москва, 2010. – С. 171–179.

3. Фергюсон Н. Практическая криптография / Фергюсон Н., Шнайер Б. – Москва : Издательский дом «Вильямс», 2011. – С. 101–114.

4. Панасенко С.П. Словарные атаки на хэш-функции. Мир и безопасность / Панасенко С.П. – Санкт-Петербург, 2010. – С. 24–31.

5. Ященко В.В. Введение в криптографию / Ященко В.В. – Москва : МЦНМО, 2012. – С. 348–350.

References

1. Petrov A. A. Kompyuternaya bezopasnost. Kriptograficheskie metody zashity / A. A. Petrov. – Moskva, 2013. – S. 448–452.

2. Lyovin V.Yu. O povyshenii kriptostojkosti odnonapravlennyh hesh-funkcij. Fundamentalnaya i prikladnaya matematika / Lyovin V.Yu. – Moskva, 2010. – S. 171–179.

3. Fergyuson N. Prakticheskaya kriptografiya / Fergyuson N., Shnajer B. – Moskva : Izdatelskij dom «Vilyams», 2011. – S. 101–114.

4. Panasenko S.P. Slovarnye ataki na hesh-funkcii. Mir i bezopasnost / Panasenko S.P. – Sankt-Peterburg, 2010. – C. 24–31.

5. Yashenko V.V. Vvedenie v kriptografiyu / Yashenko V.V. – Moskva : MCNMO, 2012. – C. 348–350.

Рецензія/Peer review : 5.6.2019 р. Надрукована/Printed :18.7.2019 р.
Стаття рецензована редакційною колегією