УДК 336.717.1:004.738.5

МЕТОД БЕЗПЕЧНОЇ ПЕРЕДАЧІ АУТЕНТИФІКАЦІЙНИХ ДАНИХ В ІНТЕРНЕТ-ПЛАТІЖНІЙ СИСТЕМІ ЗА ДОПОМОГОЮ КАСКАДНО-КОМБІНАЦІЙНОГО ХЕШУВАННЯ.

THE METHOD OF SAFE TRANSMISSION THE AUTHENTICATION DATA IN INTERNET PAYMENT SYSTEM WITH THE HELP OF CASCADE-COMBINATIONAL HASHING

Аліна Анатоліївна ЗАСЯДЬКО
доктор технічних наук, доцент, професор кафедри вищої математики та інформаційних технологій Черкаського інституту банківської справи Університету банківської справи Національного банку України (м. Київ)

Alina A. ZASYAD'KO
Doctor of Technical Sciences, Professor of Higher Mathematics and Information Technology Department, Cherkasy Institute of Banking of the University of Banking of the National Bank of Ukraine (Kyiv)

Сергій Степанович КОРОЛЮК
кандидат фіз.-мат. наук, доцент, доцент кафедри вищої математики та інформаційних технологій Черкаського інституту банківської справи Університету банківської справи Національного банку України (м. Київ)

Sergiy S. KOROLYUK
PhD in Physics and Mathematics, Associate Professor of Higher Mathematics and Information Technology Department, Cherkasy Institute of Banking of the University of Banking of the National Bank of Ukraine (Kyiv)

Оксана Володимирівна КЛЮВАК
фахівець 2-ої категорії наукового відділу Львівського інституту банківської справи Університету банківської справи Національного банку України (м. Київ)

Oxana V. KLOVAK
Specialist of the Second Category, Scientific Department of Lviv Institute of Banking of the University of Banking of the National Bank of Ukraine (Kyiv)

Анотація. Проаналізовано механізм аутентифікації в інтернет-платіжній системі на основі коду власника платіжної картки, згенерованого банком-емітентом, та запропоновано застосування каскадно-комбінаційного хешування аутентифікаційних даних.

Summary. The article dwells on the mechanism of authentication in Internet payment system based on cardholder's code generated by the issuing bank. Suggested is the use of cascade- combinational hashing of authentication data.

Ключові слова: *Інтернет-платіжна система, Інтернет-транзакція, банківська платіжна картка, аутентифікаційні дані, аутентифікація, хеш-код, алгоритм конкатенації, КСХ (код схеми хешування), каскадно-комбінаційне хешування (ККХ), ОВК (онлайн власний код).*
Key words: *Internet payment system, online transaction, banking payment card, authentication data, authentication, hash code algorithm concatenation, hash code scheme, cascade-combinational hashing, online own code.*

Постановка проблеми. Дані, які передаються власником банківської картки через Інтернет, повинні володіти трьома базовими властивостями: цілісністю, конфіденційністю та автентичністю. На нашу думку, резонним є зосередити свою увагу на аналізі схеми аутентифікації та на

процесі хешування, як на найбільш ефективному методі безпечної передачі аутентифікаційних даних. Насьогодні розроблено достатньо велику кількість протоколів аутентифікації, які базуються на використанні хеш-функцій. І хоча хешування є операція незворотна, що відповідно убезпечує від розшифрування вихідного коду зловмисником при перехопленні повідомлення, проте існує імовірність отримання однакового результату при різних вхідних даних. Існування колізій у хеш-функціях знижує надійність протоколів аутентифікації. Тому удосконалення схем хешування у протоколах аутентифікації є надзвичайно актуальним питанням.

Аналіз останніх досліджень та публікацій. Дослідженнями у галузі захисту інформації в копм'ютерних системах та мережах в Україні займаються науковці А. А. Кузнецов, С. П. Євсєєв, Б. П. Томашевський, Ю. И. Жмурко. Аутентифікацію в інтернеті досліджують такі російські учені, як Ю. А. Семенов, А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов та інші. Серед інших іноземних авторів, які досліджують хеш-функції та протоколи аутентифікації, які базуються на них, можна виділити наступних: William Stallings, Man Young Rhee, Sugata Sanyal, Ayu Tiwari and Sudip Sanyal, V. Pasupathinathan, J. Pieprzyk, H. Wang and J.Y. Cho, Sungwoo Kang, Haeryong Park, Donghyeon Cheon, Kilsoo Chun, Jaeil Lee та інші.

Мета статті полягає в аналізі схеми аутентифікації на основі спеціального коду, який генерується банком-емітентом для власника банківської картки, а також в обґрунтуванні застосування каскадно-комбінаційної схеми хешування аутентифікаційних даних в інтернет-платіжній системі.

Обґрунтування отриманих наукових результатів. Наш підхід до схеми аутентифікації в інтернет-платіжній системі базуватиметься на використанні спеціального коду (назвемо його ОВК - онлайн власний код), який генерує банківська установа покупця, та використовується лише для при здійсненні розрахунків в інтернеті.

ОВК, який згенерований банком клієнта, вводиться у полі замовлення замість реквізитів картки. Цей код є прив'язаним до карткового рахунку. Таким чином, ми уникаємо безпосередньої передачі реквізитів картки від покупця до продавця. Сервер продавця надсилає запит до процесингового центру банку клієнта щодо правильності коду, який заздалегідь був розшифрований алгоритмом хешування.

Безпечна передача коду здійснюється шляхом хешування. При звичайному хешуванні і банку, і клієнту відомі і код, і хеш-функція, якою здійснюється формування хеш-коду, а відтак - банк може перевірити присланий захешований код шляхом зіставлення із тим, який був отриманий шляхом проведення таких самих дій з тим самим кодом на стороні банку. Це звична усталена практика. Оскільки хешування є операція незворотна, це убезпечує від розшифрування вихідного коду зловмисником, якби він навіть перехопив захешоване повідомлення. З іншого боку, хешування представляє собою згортку початкової інформації, тобто існує хоча і мізерна, але таки існує імовірність отримання однакового результату при різних вхідних даних. Дану імовірність можна зменшити ще на декілька порядків при застосуванні нашої схеми комбінаційно-каскадного хешування. Інша причина введення цієї схеми – значне підвищення складності результуючого коду, що ускладнює дії зловмисника над ним. Крім того, комбінаційно-каскадне хешування дозволяє поглибити диференціацію персонального ідентифікуючого матеріалу платника. Теоретично можна навіть допустити однаковий код при різних конфігураціях хешування [1, 2].

Каскадно-комбінаційний тип хешування на вході отримує два елементи даних:

– Сам код, який має бути захешовано та передано на іншу сторону;

– Код схеми хешування.

Крім коду платник отримує ще одну зі схем комбінаційно-каскадного хешування. Цю схему також знає приймаюча сторона, отож вона не передається при пересиланні захешованого коду при здійсненні трансакції. Хешування за такою схемою передбачає використання одночасно 9 хеш-функцій (RSHash, JSHash, PJWHash, ELFHash, BKDRHash, SDBMHash, DJBHash, DEKHash, APHash). При цьому кожна з них отримує на вході одне і теж, в даному випадку, код ОВК, представлений в текстовому виді. Результати усіх функцій конкатенуються у єдине 288 бітове поле (кожна функція генерує 4 байтове число, отож при конкатенації результатів дев'яти функцій утворюється поле довжиною 36 байт). Те, в якій послідовності викликаються згадані функції, визначається кодом схеми хешування. КСХ представляє собою текстову стрічку довжиною 9 байтів, кожен символ якої ідентифікує одну певну хеш-функцію. Символи не повинні повторюватись. Відповідність між кожною функцією та її ідентифікатором наведені в таблиці 1.

Наприклад, якщо КСХ має вигляд RJPEBSDKA, то результуючий захешований код матиме такий вигляд:

RSHash(ОВК) & JSHash(ОВК) & PJWHash(ОВК) & ELFHash(ОВК) & BKDRHash(ОВК) & SDBMHash(ОВК) & DJBHash(ОВК) &

Таблиця 1

Відповідність елементів стрічки CascadeArr (див. Лістинг 1) певній хеш-функції

Символ КСХ	Хеш-функція
R	RSHash
J	JSHash
P	PJWHash
E	ELFHash
B	BKDRHash
S	SDBMHash
D	DJBHash
K	DEKHash
A	APHash

DEKHash(ОВК) & APHash(ОВК), де & - операція конкатенації.

Зрозуміло, що при здійсненні автентифікації обидві сторони транзакції повинні бути здатні розрахувати хеш-код каскадним методом, описаним вище. Одна сторона генерує його і відправляє його іншій, а та, в свою чергу, отримавши його, мусить згенерувати заново, і звірити з отриманим. Тільки повна тотожність обох стрічок є умовою для успішного проходження автентифікації.

Оскільки, генеруватись хеш-код має однаково, обидві сторони мають у своєму розпорядженні однаковий програмний модуль для обчислення. Для зручності використання в рамках різних програмних систем даний модуль скомпонований у виді динамічної бібліотеки (hashCascade. dll). Програмна система за рахунок виклику відповідного метода бібліотеки може отримати потрібний код, використавши на вході ОВК та КСХ. Місце бібліотечного модуля хешування в загальному процесі хешування можна схематично зобразити так:

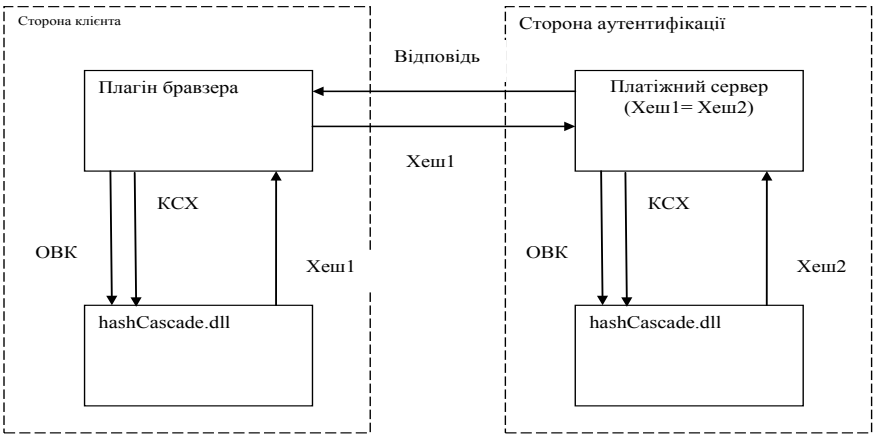

Рис.1 Пропонована програмна схема аутентифікація на основі ККХ в інтернет-платіжних системах

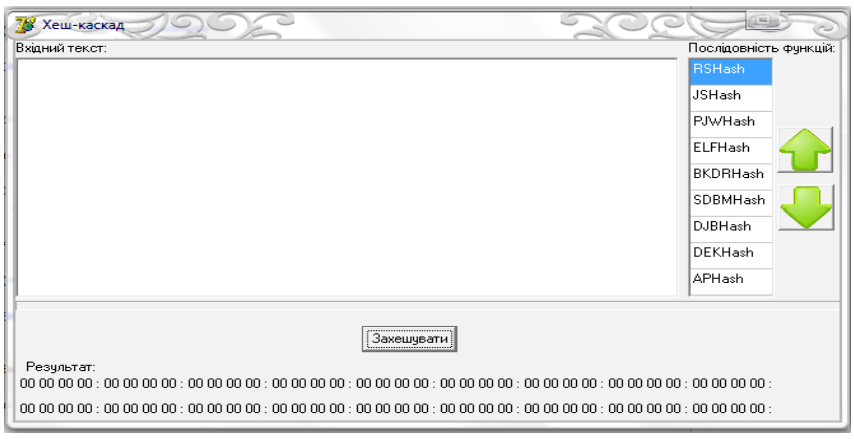

Рис. 1 Початковий вигляд вікна тестової програми

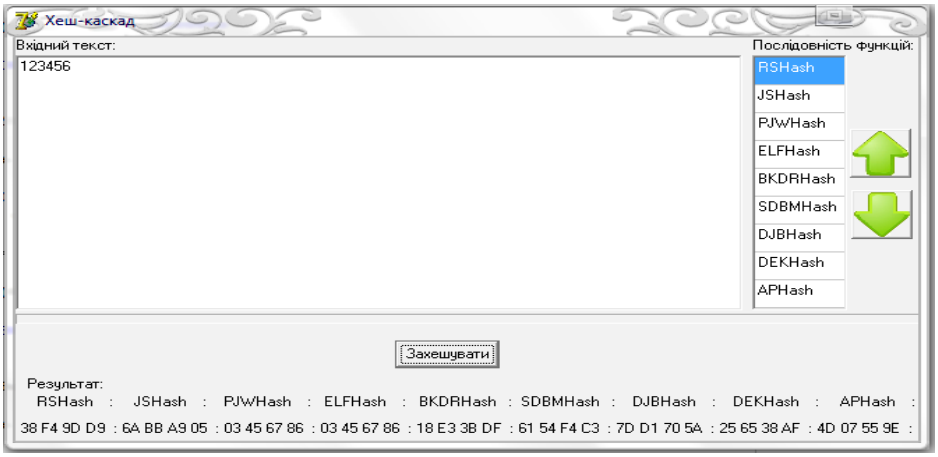

Рис. 2 Вигляд захешованого ОВК після проведенного тесту

Програмний інтерфейс модуля hashCascade.dll складається з єдиної функції, яка на вході отримує обидва параметри комбінаційно-каскадної схеми хешування (ОВК та КСХ), а на виході містить стрічку згенерованого хеш-коду [1, 2, 3].

Оскільки суть каскадно-комбінаційного хешування полягає у тому, що хеш-функції викликаються не у сталій послідовності, а в тій послідовності, яка визначається схемою комбінаційного хешування. Тому виклики даних функцій організовані не як статичні виклики, а й як виклики змінної типу функція. При виконанні хешування перебирається увесь ланцюжок схеми хешування (стрічка CascadeArr функції GetHashCode), і кожному елементу цієї стрічки знаходиться відповідна хеш-функція (див. табл. 1). Після цього найзручніше взяти адресу даної хеш-функції та викликати її за цією адресою. Така схема дозволяє легко організувати перебір усіх функцій в одному циклі. Результати викликів всіх хеш-функцій конкатенується в єдину 36 байтову стрічку, яка повертається з бібліотеки як результат [4, 5].

Щоб наочно продемонструвати, який матиме вигляд ОВК після хешування, ми розробили тестову програму. Нашу розробку можна застосовувати як додаток до інтернет-платіжної системи у форматі * .dll. (Рис. 1, 2).

Висновки. На нашу думку, найефективніший механізм аутентифікації в інтернет-платіжній системі передбачає:

1) Використання спеціального коду (онлайн власний код), який генерує банк покупця та робить прив'язку до карткового рахунку, що дає можливість не передавати реквізитів картки через Інтернет безпосередньо продавцеві.

2) Цей код можна змінювати щоразу для нової транзакції, що передбачає значні затрати для банківської установи та створення окремого підрозділу для постійного супроводження та генерування кодів, необхідність для клієнта щоразу звертатися до свого банку за новим кодом. Проте цей код можна не змінювати щоразу для кожної нової транзакції шляхом його хешування у процесі передачі. У нашій статті ми пропонуємо застосовувати каскадно-комбінаційне хешування аутентифікаційних даних.

Список використаних джерел

1. Исследование протоколов и механизмов защиты информации в компьютерних системах и сетях [Текст] / А. А. Кузнецов, С. П. Евсеев, Б. П. Томашевский, Ю. И. Жмурко // Збірник наукових праць Харківського Університету Повітряних Сил ім. І. Кожедуба. — 2007. — №2(14) . — С. 102–111.

2. [Електронний ресурс]. — Режим доступу : http://ru.wikipedia.org/wiki/N-Hash

3. Credit Card Encryption and Password Hashing Utility Component [Електронний ресурс]. — Режим доступу : http://www.caritas.org.au/Content/NavigationMenu/Caritas_Documents/PDFs/asiUtil_CreditCardEncryption.pdf

4. Семенов Ю. А. Аутентификация в Интернет [Електронний ресурс] / Ю. А. Семенов. — Режим доступу : http://docs.luksian.com/networks/techs/intro/?f=./6/authent.

shtml

5. Guidelines: Authentication in an Internet Banking Environment, Federal Financial Institutions Examination Council, Arlington, October 2005, [Електронний ресурс]. — Режим доступу : http://www.ffiec.gov