УДК 336.717.1:004.738.5

Клювак О. В.

МЕХАНІЗМ БЕЗПЕЧНОЇ ПЕРЕДАЧІ АУТЕНТИФІКАЦІЙНИХ ДАНИХ В ІНТЕРНЕТ-ПЛАТІЖНИХ СИСТЕМАХ

Анотація. У статті описана схема аутентифікації в Інтернет-платіжних системах та запропоновано каскадно-комбінаційне хешування даних під час розрахунків банківською карткою в Інтернеті.

Ключові слова: Інтернет-платіжна система**,** Інтернет-транзакція, банківська платіжна картка (БПК)**,** аутентифікаційні дані, аутентифікація, хеш-код, алгоритм конкатенації, КСХ (код схеми хешування), каскадно-комбінаційне хешування (ККХ), ОВК (онлайн власний код).

Вступ. В умовах глобалізації фінансових ринків при здійсненні купівлі-продажу товарів та послуг в режимі реального часу основною причиною для занепокоєння є шахрайські операції, зокрема. з банківськими платіжними картками. Саме тому десятки тисяч власників Інтернет-магазинів перебувають у пошуку надійної технології, яка б забезпечила захист від шахрайства та мала б загальновизнану репутацію у галузі електронної комерції, а покупці – в очікуванні того, що зможуть без будь-яких хвилювань за свої кошти здійснювати платежі в Інтернеті. Високий рівень шахрайства в Інтернеті являється фактором уповільнення розвитку електронної комерції, адже покупці, продавці та банки остерігаються використовувати дану технологію через небезпеку понести фінансові втрати.

Метою статті є аналіз механізму безпечної передачі аутентифікаційних даних в Інтернет-платіжних системах на основі хешування .

Постановка завдання. Для забезпечення фінансової стійкості, інформація, яка передається через Інтернет під час здійснення платежів, повинна володіти трьома базовими властивостями цілісністю, конфіденційністю та автентичністю. На нашу думку, резонним є зосередити свою увагу на аналізі схеми аутентифікації та на процесі хешуванні, як на найбільш ефективному методі безпечної передачі аутентифікаційних даних. На сьогоднішній день розроблено достатньо велику кількість протоколів аутентифікації, які базуються на використанні хеш-функцій. Тому удосконалення схем хешування у протоколах аутентифікації є надзвичайно актуальним питання.

Результати. Щоб проаналізувати безпечну схему Інтернет-транзакції, розглянемо способи захисту повідомлень при використанні хеш-коду (Рис. 1, де К- симетричний ключ, H (M) - хеш-код, M - повідомлення) [1, 2].

Можна також зашифрувати не лише хеш-код, але й саме повідомлення. У цьому випадку забезпечується цілісність, аутентифікація та конфіденційність (тільки сторони A і B знають K). Фактично у цьому полягає механізм використання цифрового підпису (Рис. 2, де KS_a - секретний ключ відправника, $КР_a$ – відкритий ключ відправника)) [1, 2].

З метою аутентифікації повідомлень можна використовувати функцію хешування без шифрування. У цьому випадку передбачається, що дві сторони використовують відоме їм секретне значення S. Відправник A обчислює значення функції хешування для результату конкатенації повідомлення X та S, та приєднює отримане значення

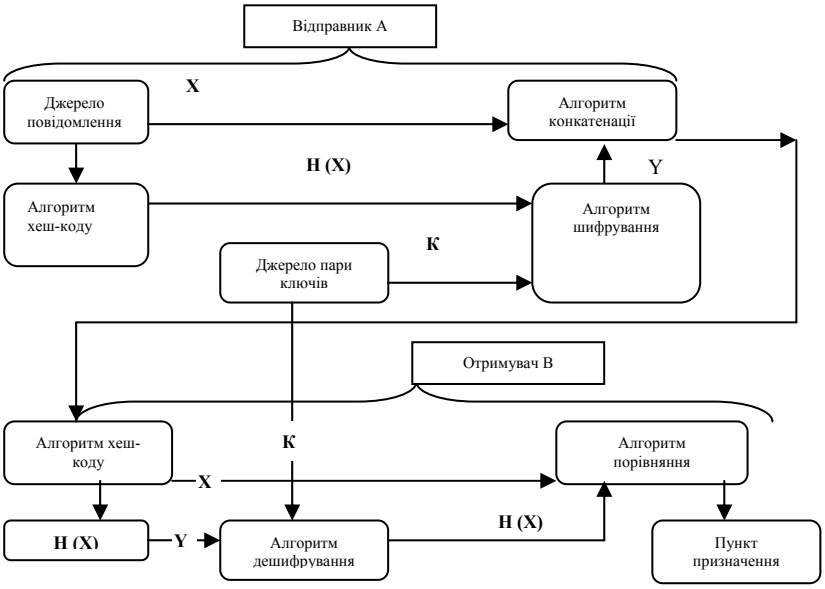

Рис. 1. Забезпечення аутентифікації на основі використання хеш-коду

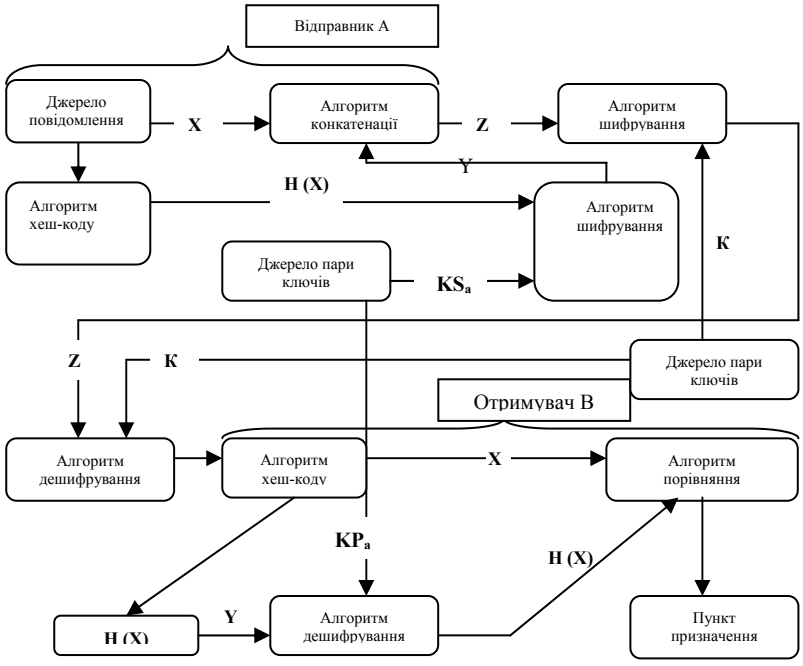

Рис. 2. Забезпечення аутентифікації, цілісності та конфіденційності на основі використання хеш-коду

функції хешування до X. Отримувачу B значення S відомо, тому він може обчислити значення функції хешування. При цьому забезпечується аутентфиікація (тільки A і B знають S) (Рис. 3) [1, 2].

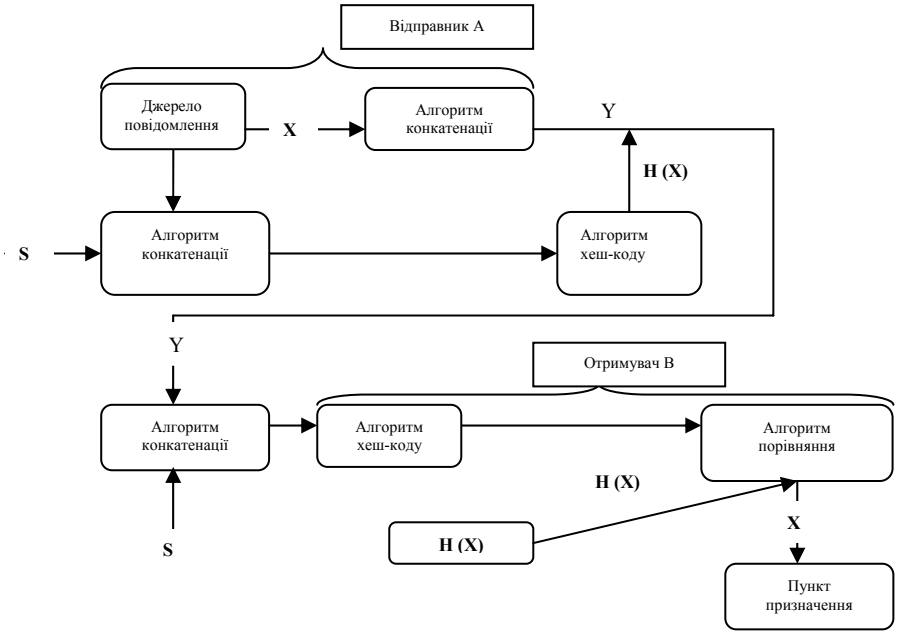

Рис. 3. Забезпечення аутентифікації на основі використання хеш-коду

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 сугубо 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. Даний код хешується у процесі передачі та на виході отримана стрічка підлягає перевірці сервером продавця. Сервер продавця надсилає запит до процесингового центру банка клієнта щодо правильності коду, який заздалегідь був розшифрований алгоритмом хешування. Також, у цьому запиті вміщені інші дані покупця, такі як прізвище, ім'я та по-батькові. Банк покупця звіряє дані та надсилає відповідь. Крім того, досить ефективним додатковим заходом безпеки є смс-сповіщення. Після того, як клієнт надіслав своє підтвердження, транзакція зараховується або відхиляється. Кошти списуються з рахунку покупця на користь продавця (Рис. 4).

При присвоєнні ОВК також відбувається присвоєння клієнту схеми хешуваня для більш захищеної її передачі. 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

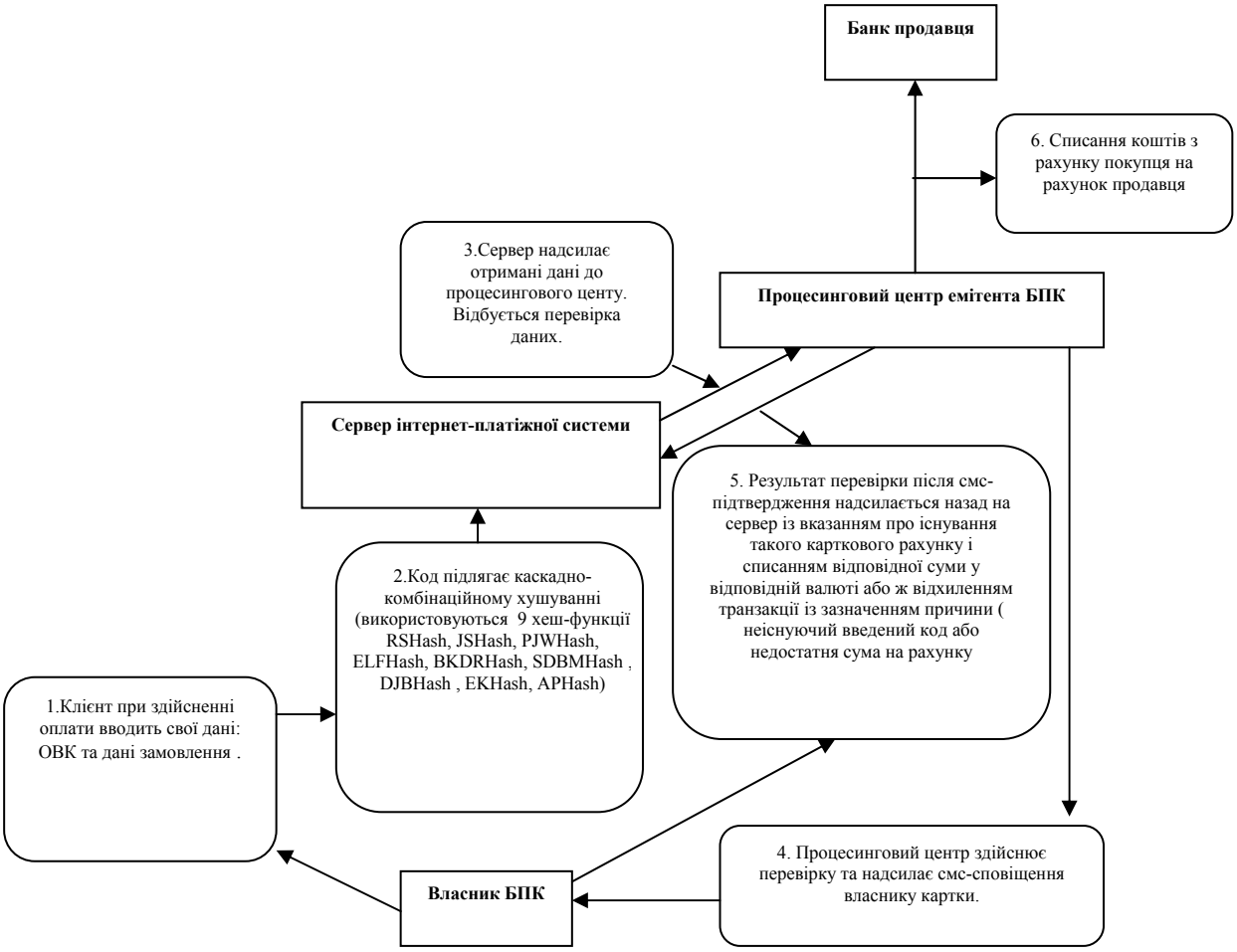

Рис. 4. Схема процесу аутентифікаціїї на основі ОВК із елементами його хешування

поглибити диференціацію персонального ідентифікуючого матеріалу платника. Теоретично можна навіть допустити однаковий код при різних конфігураціях хешування.

Комбінаційно-каскадне хешування, яке ми пропонуємо застосовувати до коду під час здійснення транзакції в інтернет-платіжній системі власником картки, полягає у наступному.

Даний 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 з схем комбінаційно-каскадного хешування. Цю схему також знає приймаюча сторона, отож вона не передається при пересиланні захешованого коду при здійсненні транзакції. 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 викликається 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.

Зрозуміло, що при здійсненні аутентифікації 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 аутентифікації.

Висновки. Тобто, на нашу думку, найефективніший механізм аутентифікації передбачає:

1) Використання спеціального коду, який генерує банк покупця, 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 генерації кодів, необхідність для клієнта щоразу звертатися до свого банку за новим кодом. Про те 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.

Література

1. Кузнецов А.А., Евсеев С.П., Томашевский Б.П., Жмурко Ю.И. Исследование протоколов и механизмов защиты информации в компьютерных системах и сетях [Електронний ресурс] - Режим доступу: http://www.nbuv.gov.ua/portal/natural/ZKhUPS/2007_2/Kuznecov.pdf
2. Семенов Ю.А. Аутентификация в Интернет [Електронний ресурс] - Режим доступу: http://docs.luksian.com/networks/techs/intro/?f=./6/authent.shtml
3. Credit Card Encryption and Password Hashing Utility Component http://www.caritas.org.au/Content/NavigationMenu/Caritas_Documents/PDFs/asiUtil_CreditCardEncryption.pdf
4. [Електронний ресурс] - Режим доступу : http://ru.wikipedia.org/wiki/N-Hash
5. Sungwoo Kang, Haeryong Park, Donghyeon Cheon, Kilsoo Chun, Jaeil Lee Requirements for e-payment system based on the credit card [Електронний ресурс] - Режим доступу http://www.iadis.net/dl/final_uploads/200406P002.pdf

Summary. The authentication scheme in Internet payment-systems is described in the article and it is proposed the mechanism of cascade-combinational hashing data during the realization online banking card transaction.

Keywords: Internet payment system, online transaction, banking payment card, authentication data, authentication, hash code algorithm, concatenation, KSH (hash code scheme), cascade-combinational hashing (CCH), OOC (online own code).

Стаття надійшла до редакції 6.04.2012