УДК 004.056.5:004.738.5

О. В. Салієва
В. В. Порицька

ПОРІВНЯННЯ ІСНУЮЧИХ ВЕРСІЙ ПРОТОКОЛУ 3-D SECURE

Вінницький національний технічний університет

Анотація

У статті наведено порівняльний аналіз існуючих версій протоколу 3-D Secure, що використовуються для забезпечення безпеки онлайн-платежів. Розглянуто принцип роботи протоколу, особливості кожної версії та відмінності в їх функціонуванні. Проаналізовано кожну версію з точки зору зручності для користувачів та ефективності запобігання шахрайству. Особливу увагу зосереджено на вдосконаленнях у 3-D Secure другої весрсії.

Ключові слова: 3-D Secure, онлайн-платежі, безпека платіжних систем, кібербезпека.

Abstract

The article provides a comparative analysis of the existing versions of the 3-D Secure protocol used to ensure the security of online payments. The principle of protocol operation, features of each version and differences in their functioning are considered. Each version is analyzed in terms of user-friendliness and fraud prevention efficiency. Particular attention is focused on improvements in 3-D Secure of the second version.

Keywords: 3-D Secure, online payments, payment system security, cybersecurity.

Вступ

З розвитком електронної комерції проблема захисту особистих даних клієнтів стає дедалі актуальнішою. Адже все більше користувачі обирають цифрові способи оплати завдяки їх зручності та швидкості. Це має особливе значення для мобільних платежів, де виникли цілі сегменти послуг, що базуються на даній технології. Однак паралельно з цим зростає загроза для онлайн-платежів, оскільки зловмисники вмотивовані постійно розробляти та вдосконалювати методи викрадення платіжних даних для отримання доступу до банківських рахунків.

Основна частина

Традиційні методи захисту, такі як CVV код чи пароль, не завжди можуть повною мірою забезпечити належний рівень безпеки. Адже часто користувачі повторно використовують паролі, що може призвести до витоку конфіденційної інформації. Тому для підвищення безпеки було вирішено розробляти додаткові протоколи забезпечення належного рівня захищеності. Одним з таких протоколів є 3-D Secure.

Перша версія протоколу була випущена наприкінці 1990-х років компаніями Visa та Mastercard та вимагала від власників карток автентифікації транзакцій за допомогою статичного пароля або одноразового пароля, надісланого через SMS або електронну пошту.

Робота протоколу базується на співпраці трьох доменів [1]:

– домена емітента, який відповідає за автентифікацію власника картки банком, що випустив платіжну картку;

– домена еквайєра, відповідального за сторону, що буде отримувати платіж;

– домена взаємодії, що використовується для забезпечення зв’язку між вищезгаданими учасниками. На практиці цю роль виконує платіжний процесор.

Процес оплати відбувається наступним чином [2]:

– покупець формує список товарів, що бажає придбати та натискає кнопку “оформити”;

– веб-сторінка ініціює запит з використанням протоколу 3-D Secure та надсилає платіжні дані до домену емітента, щоб автентифікувати покупця;

– банк-емітент перевіряє отриману інформацію на достовірність та у результаті надсилає відповідь щодо дозволу проведення платежу;

– якщо банк-емітент дозволив проведення платежу, клієнта буде переведено на іншу сторінку, де необхідно ввести пароль;

– отриманий пароль знову перевіряється банком-емітентом;

– якщо пароль правильний, то продавцю надсилається код авторизації, що підтвердить особу користувача;

– банк-еквайер завершує фінансову операцію, після чого покупка завершена.

Хоча цей протокол ефективно виконує свою основну функцію – підтвердження особи покупця, на практиці він може спричинити ризик відмови від покупки обраного товару. Це пов'язано з необхідністю введення даних на зовнішній сторінці, яка не завжди викликає довіру у користувача. Також дану версію неможливо використати у мобільних додатках, адже використовується протокол XML. Тому користувачам все одно доводиться виходити із застосунку і заходити у браузер, щоб підтвердити платіж. Зважаючи на вказані недоліки досить швидко виникла потреба в удосконаленні можливостей даного протоколу.

У 2016 році було представлено другу версію протоколу зі значними перевагами. Зокрема, статичні паролі замінили токенами та біометричними даними, що дозволило підвищити надійність авторизації та покращити користувацький досвід. Крім того, друга версія дозволила здійснювати перевірку транзакцій безпосередньо в мобільних додатках, усуваючи необхідність переходу до сторонніх застосунків. Це стало можливим завдяки тому, що замість перенаправлень клієнтів на зовнішні сторінки, почали використовувати API. Також дана версія протоколу дозволяє використовувати єдиний стандарт безпеки незалежно від того, яка платформа використовується клієнтом [3].

Варто зазначити вдосконалення, що стосуються управління ризиками. Адже, коли веб-сторінка ініціює новий платіж, надсилаються не лише платіжні дані, а й багато додаткових, для оцінювання ризику. Таким чином забезпечується ризик-орієнтована автентифікація (Risk-Based Authentication), яка виконується на сервері контролю доступу (Access Control Server) [4].

Основні відмінності між версіями протоколу 3-D Secure відображено у таблиці 1.

Таблиця 1 – Порівняння існуючих версій протоколу 3-D Secure

Ключові особливості	Версія протоколу	
	3-D Secure 1	3-D Secure 2
Автентифікація	Статичний або одноразовий пароль	Біометрія, токенти, push-сповіщення
Взаємодія з клієнтами	Часті перенаправлення на сторінку банку, незручний користувацький інтерфейс	Вбудована аутентифікація без пересилань, зручний користувацький інтерфейс
Підтримка мобільних пристроїв	Погана підтримка мобільних платежів, неадаптовані сторінки	Інтеграція з мобільними додатками, SDK для розробників
Управління ризиками	Відсутній аналіз ризиків, високий рівень відхилень	Ризик-орієнтована автентифікація (RBA), мінімізація незручностей для користувачів

Варто зазначити, що завдяки застосуванню RBA при низькому рівні ризику, клієнт може пройти лише фонову автентифікацію без подальшої перевірки, що значно спрощує процес оформлення товарів для покупців. Якщо ризик буде високим, то клієнт все одно повинен буде пройти процес додаткової автентифікації для гарантування високого рівня безпеки

Таким чином, на сьогоднішній день друга версія протоколу відповідає міжнародним стандартам та широко використовуються у повсякденному житті.

Висновок

У дослідженні проведено аналіз різних версій протоколу безпеки онлайн-платежів 3-D Secure, описано ключові відмінності між ними. Показано, що друга версія протоколу забезпечує підвищений рівень захисту та покращену зручність для користувачів. В свою чергу, автентифікація на основі оцінювання ризиків дозволяє зменшити кількість зайвих перевірок. Загалом досягається оптимальне поєднання безпеки та зручності використання, що сприяє зниженню відмов від покупок і підвищенню довіри до онлайн-транзакцій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Mamonova H., Lysenko M. History of creation and development of 3DS-technology. *Modeling and information systems in economics*. 2022. № 102. С. 158–170. URL: https://doi.org/10.33111/mise.102.13 (дата звернення: 09.02.2025).
2. Channing Lovett. What is 3D secure authentication? How does it work? | airwallex. *Airwallex: Trusted Global Payments & Financial Platform*. URL:https://www.airwallex.com/blog/what-is-3d-secure-authentication#What_is_3D_Secure_authentication? (дата звернення: 09.02.2025).
3. 3D secure 2: stronger authentication & support for mobile customers URL: https://www.shift4.com/blog/3d-secure-2-stronger-authentication (дата звернення: 10.02.2025).
4. Visa 3-D secure 2.0. URL: https://rs.visa.com/content/dam/VCOM/global/run-your-business/documents/visa-3d-secure-2-infographic.pdf (дата звернення: 10.02.2025).

Порицька Вероніка Володимирівна – студентка групи 1КІТС-21б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: porickaveronika@gmail.com

Науковий керівник: ***Салієва Ольга Володимирівна*** – доктор філософії за спеціальністю 125 «Кібербезпека», доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: salieva8257@vntu.edu.ua

Porytska Veronika Volodymyrivna – student of group 1KITS-21b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: porickaveronika@gmail.com

Scientific supervisor: Saliieva Olha Volodymyrivna – Doctor of Philosophy in specialty 125 "Cybersecurity", Associate Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: salieva8257@vntu.edu.ua