УДК 336.717.13..004.738.5

О.В. Клювак

Університет банківської справи Національного банку України, Львів

МЕХАНІЗМ ДІЇ ПЕРЕМИКАЧА ПЛАТЕЖУ ЯК ЗАСОБУ ПІДВИЩЕННЯ РІВНЯ БЕЗПЕКИ В ЕЛЕКТРОННІЙ КОМЕРЦІЇ

У розгляді загальної схеми інтернет-платежів, так і у процедурі аутентифікації у цій схемі, важливим є введення поняття перемикача цих же платежів. Існуючі комерційні системи розроблені таким чином, щоб продавці могли працювати без додаткового ризику. Наприклад, в зазвичай у системі платежів за допомогою карток банк-емітент бере на себе ризик, пов'язаний із зловживаннями карткою, якщо продавець підпорядковується встановленому протоколу прийняття картки. Стандартні протоколи прийняття можуть включати у себе перевірку підпису власника картки та перевірку законності її використання у режимі реального часу. Проте при комерційних операціях в мережі продавець фізично не може перевірити картку покупця і цей ризик зводиться для продавця до так званої комерційної операції «картка не представлена». Багато продавців не можуть взяти на себе такий ризик у зв'язку із обмеженістю їх фінансових ресурсів. Розв'язанням цієї проблеми може бути створення мережевої служби платежів, при якій зменшується ризик шахрайства в мережі, що дає можливість більшій кількості продавців приймати участь у комерційних операціях. Перемикач платежу представляє собою мережеву послугу, за допомогою якої санкціонуються і виконуються цифрові платіжні доручення, забезпечені зовнішніми рахунками. Перемикач платежу посвідчує замовлення, перевіряє наявність достатніх коштів, а згодом починає операцію по переказу коштів для виконання платіжного доручення. В даній мережі може існувати не один перемикач платежу. Системи введення мережевих замовлень виконують ідентифікацію рахунків банківських карток, які використовуються для платежів. В більшості випадків операції формування замовлень не зашифровуються, і саме тому можуть бути перехоплені. Тому, резонним було б забезпечувати захист комунікацій для введення замовлень за допомогою криптографічних протоколів. Зазвичай навіть при наявності криптографічних протоколів, мережеві засоби, такі як робочі станції, підпадають під ризик з боку програмного забезпечення клієнта та використання викрадених банківських карток.

Існуючі сервери платежів не пов'язані із фінансовою системою для ідентифікації платежів або не забезпечують надійної ідентифікації у реальному часі, що безпосередньо необхідно на серверах продавців. Сервери платежів повинні забезпечувати довір'я між учасниками операцій, а також учасники повинні довіряти серверу платежів, а сервер у свою чергу повинен бути включеним у процес

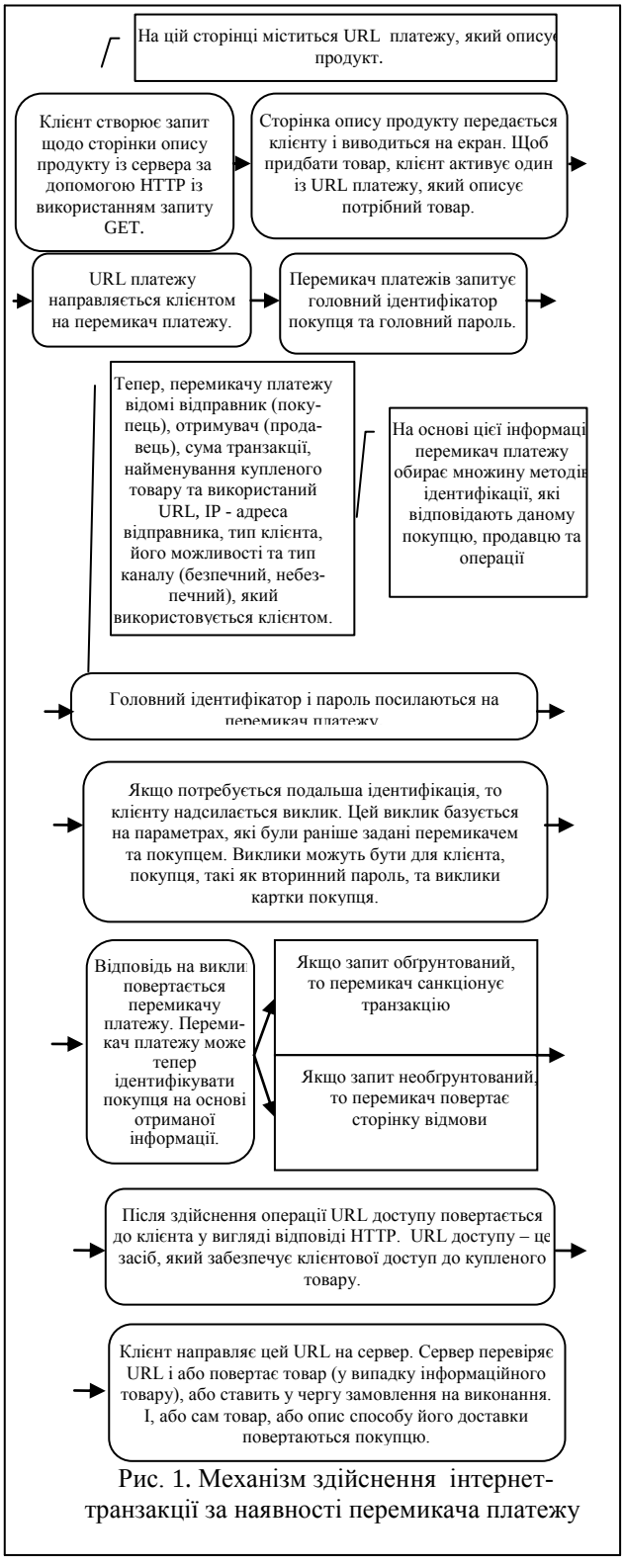

Рис. 1. Механізм здійснення інтернет-транзакції за наявності перемикача платежу

здійснення транзакції. Основною особливістю системи анонімних платежів, котра повинна захищати учасників від будь-яких зловживань, є ретельний поділ інформації, так, щоб кожному учасникові була доступна лише необхідна інформація. Іншим сервером платежів є сервер, який виділяє кожному користувачеві рахунок із унікальним ідентифікатором. При купівлі товару споживач дає ідентифікатор продавцю. Продавець повідомляє про операцію на сервер, який у свою чергу надсилає електронну пошту споживачу з проханням підтвердити операцію. Споживач може прийняти операцію, відмінити платіж або повідомити про шахрайство. При цьому продавець піддається ризику, оскільки покупець може відмінити платіж [1, 2].

У перемикачі платежів використовується кілька методів ідентифікації, і ці методи використовуються в залежності від типу транзакції та її суми. Щоб визначити, який метод необхідно застосувати, використовується багаторівневий підхід. Він забезпечує баланс між безпекою та зручністю для користувача і дозволяє забезпечення виконання потрібних функцій у випадку невдачі одного з методів.

Перемикач платежів містить систему автоматичної підтримки користувача, яка забезпечує інформацію про здійснені операції комерційних платежів. У перемикачі платежів знаходиться повний список всіх операцій, і, таким чином, забезпечується фіксована точка доступу до купівлі товарів, дозволяючи користувачу переглядати детальну інформацію про комерційні операції і заповнювати форми автоматичного обслуговування покупців. У випадку переривання зв'язку під час транзакції користувач має можливість визначити, в якому стані знаходиться операція.

При звичайній операції купівлі можуть використовуватися десять повідомлень. На рис. 1 подана схема здійснення платежу на основі перемикача платежів. У ній фігурує поняття URL-платежу. URL-платіж являє собою рядок, у якому містяться наступні дані: ім'я вузла перемикача платежу; ідентифікатор продавця; ціна продукту та валюта; цільовий URL для доставки продукту; термін дії платіжного URL; аутентифікатор (цифровий підпис на платежі URL, отриманий із використанням особистого ключа продавця). Також невід'ємним поняттям у вищезазначеній схемі є URL доступу. Складовими частинами URL доступу є: ім'я сервера та ідентифікатор товару, посвідчення покупця, IP – адреса (адреса покупця включається для обмеження URL доступу наданням інформації лише по заданій адресі IP), термін закінчення дії URL, посвідчення URL – доступу (цифровий підпис, який відноситься до всього URL та дозволяє серверу переконатися, що даний URL був створений за допомогою перемикача платежів.

Авторизація виконується у відповідності із фінансовим інструментом, який підтримує рахунок покупця і включає компонент заданого перемикача і компонент зовнішньої фінансової системи. Санкціонування із використанням перемикача включає файлові перевірки, основну множину лімітів та дозволені коди товарів, перевірку адреси, перевірку швидкості та перевірки, специфічні для типу рахунку. Якщо транзакція пройшла усі перевірки перемикача, то вона направляється на зовнішні фінансові організації, які несуть відповідальність за засоби платежу, пов'язані із рахунком покупця (рис. 1) [3, с. 401-404].

Таким чином, перемикач платежу є надзвичайно важливим компонентом у схемі здійснення безпечних інтернет-транзакцій та розробляється для виконання мікроплатежів на основі банківських карток. Також, прерогативою такого сервісу є об'єднання декількох типів сертифікації для одного і того ж фінансового інструмента з метою зменшення навантаження на зовнішні фінансові мережі та покращення продуктивності системи. При такому об'єднанні перемикач платежу може авторизувати транзакцію без звернення до зовнішніх фінансових систем. Якщо транзакція неавторизована, то покупцю повертається сторінка відмови. Якщо операція авторизована, то вона вноситься у протокол виконання, після чого вважається виконаною.

Список літератури

1. Пол Джонс, Армайндер Кеюр О безопасности электронной коммерции [Електронний ресурс]. – Режим доступу до док.: http://www.iso.ru/journal/articles/86.html.

2. E-Commerce Gateway merchant interface [Електронний ресурс]. – Режим доступу до документу: st.freelance.ru/users/al/alexglazkov/upload/f_49cb3932d452b.doc.

3. Вакка Дж. Секреты безопастности в Internet. – К.: Диалектика, 1997. – 512 с., ил