УДК 004.94

ПавлоСтрубицький, к.т.н., доцент, КатеринаПришляк, викладач-стажист
Тернопільський національний економічний університет

АНАЛІЗ ПЛАТІЖНИХ СИСТЕМ ЗА ДОПОМОГОЮ ІМІТАЦІЙНОЇ МОДЕЛІ

Запропоновано нову відмовостійку он-лайн електронну платіжну систему. На основі методу Монте-Карло проведено моделювання поведінки системи електронних платежів, яке дозволило провести аналіз впливу різних факторів на швидкість проведення платежів. Після аналізу всіх можливих сценаріїв відмов, у кожному конкретному випадку пропонується рішення, яке базується на механізмах відкату і відновлення.
Ключові слова: імітаційна модель, платіжна система, відмовостійкість.

Pavlo Strubytskyi, Kateryna Pryshliak
ANALYSIS PAYMENT SYSTEMS USING A SIMULATION MODEL.

Failover A new online electronic payment system. Based on Monte Carlo Simulation conduct electronic payment system that allowed an analysis of various factors on the rate of payments. After analyzing all possible scenarios of failures in each case the proposed solution, which is based on the rollback and recovery mechanisms.
Keywords: A simulation model, payment systems, fault tolerance.

Основна відмінність між он-лайн і оф-лайн електронними платіжними системами полягає в тому, що протокол оплати у випадку он-лайн системи контролюється, перевіряється і авторизується довіреною третьою стороною. В автономних системах оплати протокол виконується тільки між клієнтом і магазином, без довіреної третьої сторони. Таким чином, цей вид електронних платіжних систем може гарантувати більшу свободу для клієнтів, ніж он-лайн системи електронних платежів, але їх головним недоліком є те, що виявлення шахрайства може відбутися тільки після оплати, на основі протоколів депозиту. Це одна з причин, чому он-лайн платіжні системи все частіше використовуються в якості автономних систем. Можна сказати, що в он-лайн електронні платіжні системи забезпечують профілактичну цілісність проведення повноцінних платежів, тоді як оф-лайн системи мають підвищений рівень небезпеки.

На сьогоднішній день реалізовано багато он-лайн систем електронних платежів, і головна мета їх розвитку полягає в забезпеченні рівня необхідної безпеки. Аналіз існуючих систем електронних платежів показав, що реальні системи мають дуже мало вбудованих механізмів відмовостійкості, або вони зовсім відсутні. Пропонується нова он-лайн система електронних платежів, яка аналогічна до існуючих (наприклад, Visa, PayPal), але забезпечує реалізацію механізмів відмовостійкості.

Запропонована он-лайн система електронних платежів використовує транзакції між трьома видами об’єктів: клієнт (платник), електронний магазин (одержувач) і банк (довірена третя сторона). Діаграма послідовностей використання даної системи електронних платежів запропонованої системи показаний на Рис 1.

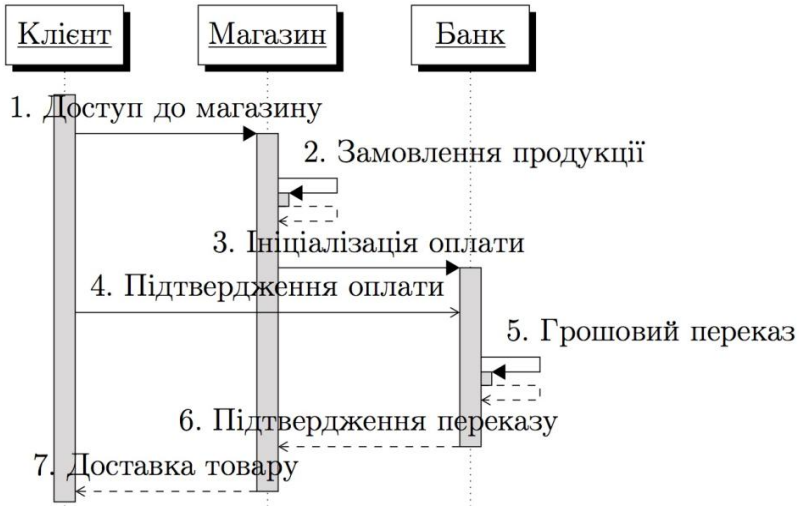

Рис. 1. Архітектура використання системи

Хронологічний порядок подій у випадку інтернет-магазину наступний:

1. Клієнт, використовуючи веб-браузер, отримує доступ до віртуального магазину.
2. Клієнт вибирає один, або кілька продуктів чи послуг магазину, використовуючи свою корзину, і запускає процес оплати.
3. Магазини збирає деяку інформацію для доставки продукції (наприклад, адресу), породжує ID транзакції, зберігає всі дані в базі даних, і перенаправляє браузер клієнта на сайт банку. Магазин відправляє у банк зашифровані ID транзакції, суму грошей і назву магазину.
4. Банк просить клієнта заповнити форму безпеки для аутентифікації: ім’я, номер кредитної картки, дата видачі, строк дії та пароль.
5. Ґрунтуючись на цих даних, банк перевіряє особу клієнта, терміну дії картки, сума грошей на рахунку, і просить клієнта підтвердити переказ грошей.
6. Якщо банк отримує підтвердження від клієнта, то перераховує запрошену і підтверджену суму грошей на рахунок магазину, зберігає угоду в базі даних, і відправляє підтвердження, використовуючи повідомлення з цифровим підписом.
7. Магазин доставляє оплачений продукт або послугу клієнтові.
8. Магазин зберігає отримані повідомлення підтвердження, які підписані банком. Це повідомлення може бути використана пізніше в якості підтвердження оплати.
9. Клієнт може будь-коли перевірити особистий архів оплати через доступ до сайту банку, використовуючи свої логін і пароль.

Дана система забезпечує анонімність, тому що клієнт не повинен подавати свої реальні особисті дані в магазин, наприклад, своє ім’я, або номер кредитної картки. Клієнт запускає платіж за допомогою банку і тільки банк може ідентифікувати його. Магазин не відправляє в банк всю докладну інформацію покупки (наприклад, перелік замовлених товарів), тільки ID транзакції і суми грошей. Таким чином, магазин не буде знати справжню особу клієнта, і банк не буде знати, що клієнт купує. Магазин знає тільки адресу доставки, і банк знає, магазин і суму грошей, яку використовує клієнт.

Для встановлення заходів необхідного рівня безпеки та стійкості до відмов, проаналізуємо в хронологічному порядку події, які можуть відбуватися в системі, щоб можна було виявити вразливі місця системи електронного платежу.

Для забезпечення безпеки основними рішеннями є:

1. Щоб уникнути небажаного доступу магазину до конфіденційних даних клієнта, пропонується використовувати перенаправлення ідентифікації клієнта та угод оплати сервером банку на сайт відповідних магазинів.

2. Для взаємного ототожнення між клієнт-банк та магазин-банк використовувати нові протоколи ідентифікації наведені в [1].
3. Зв'язки магазин-банк і клієнт-банк проводити у зашифрованому вигляді (Open SSL).

Для забезпечення відмовостійкості проаналізовано всі можливі сценарії відмов і для кожного випадку пропонується рішення, яке базується на механізмах відкату та відновлення.

На основі методу Монте-Карло було проведено моделювання поведінки системи, для того, щоб отримати порівняння ефективності системи електронних платежів з забезпеченням відмов у порівнянні з системою, яка не обробляє втрати зв'язків між клієнтом і банком та магазином і банком. Для цього визначимо події «успіх» і «збій» по відношенні послуг, які надаються електронною платіжною системою:

$$Sucess = (payment \wedge devivery) \vee (\overline{payment} \wedge \overline{devivery}),$$

$$Malfunction = (payment \wedge \overline{delivery}) \vee (\overline{payment} \wedge delivery)$$

Щоб заповнити таблиці істинності для "SuccessU" (успіх в простій системі) і "SuccessT" (успіх у відмовостійкій системі) при роботі системи в цілому, проаналізуємо архітектуру послідовностей роботи системи. Усі можливі ситуації збоїв у випадках втрати повідомлень між об'єктами або помилковими повідомленнями можна згрупувати у вигляді таблиці. При аналізі використано чотири логічних змінні M_1, M_2, M_3 і M_4\{ Mi = 1 – доставлене повідомлення, Mi = 0 – втрачене або помилкове повідомлення), які описують основні зв'язки між ооб'єктами платіжної системи: Mi – клієнт-магазин; M_2 – магазин-банк; M_3 – клієнт-банк; M_4 – банк-магазин.

Проаналізувавши отримані дані можна спостерігати цікаву річ: перша змінна не впливає на значення двох функцій. Це можна пояснити тим, що операції людини можна розглядати у будь-якому випадку як «відмовостійкий фактор» – вона може повторити свої останні виконані дії, або може переслати повідомлення, або навіть може запоповнити відповідну форму заново. Змінні M_2 і M_4 описують той же канал зв'язку, тільки напрямок повідомлень відрізняється. Алгоритм обчислення успішності в обох випадках використовує три змінні M_2, M_3 і M_4.

Програмна реалізація моделі генерує послідовно різні випадки збоїв в системі на двох ділянках: магазин-банк і клієнт-банк, сканування всіх наявних можливостей. Для кожної обраної комбінації типу shoprate – clientbankmessagelossrate, програма багаторазово обчислює значення функцій f1 = successUi f2 = successT, відповідно, за допомогою генератора випадкових чисел.

Можна спостерігати 10% збільшення швидкості успіху операцій в відмовостійкої випадку, в основному викликані успішим уникненням збоїв, що виникли в стороні клієнта.

Література.

1. Poszet O., Vári-Kakas S., Novac O., Drăgan H., Ignat I.: Efficiency of Identification Protocols in Electronic Payment Systems, Annals of the University of Oradea, Volume Electrotechnics, Session Computer Science and Control Systems, 2005, pp. 118-121