НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Звіт з виконання комп'ютерного практикуму

ДОСЛІДЖЕННЯ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ СИСТЕМИ PAYPAL

Виконали студенти
групи ФІ-32мн
Мельник Ілля,
Міснік Аліна

Перевірила:
Селюх П.В.

Київ — 2024

Мета роботи: проаналізувати побудову платіжних систем та їх основні характеристики, обґрунтувати їх захищеність та вибір криптографічних примітивів.

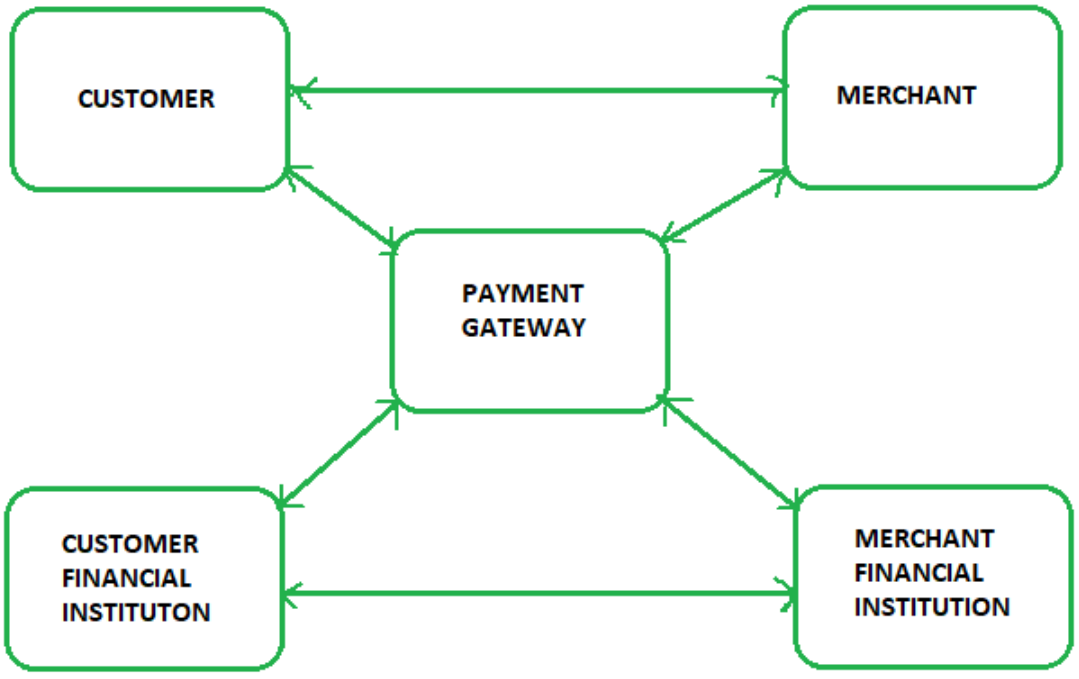
Постановка задачі: дослідити особливості реалізації криптографічних протоколів, а також особливості роботи з електронними гаманцями системи PayPal.

1 ХІД РОБОТИ

1.1 Загальні теоретичні відомості побудови платіжних систем та їх основні характеристики

Одним з сучасних методів забезпечення захисту платежів є протоколи безпечної транзакції специфікації SET.

Але перш ніж обговорювати SET, розглянемо загальний сценарій електронних транзакцій, який включає клієнта, платіжний шлюз, фінансову установу клієнта, продавця та фінансову установу продавця. Цю схему можна побачити на малюнку нижче.



Метод SET (Security Electronics Transaction) заснований на використанні цифрових сертифікатів відповідно до стандарту X.509. Secure Transaction Protocol SET – це стандарт, розроблений MasterCard і VISA при значній участі IBM, GlobeSet та інших партнерів. Це дозволяє користувачам

купувати товари в Інтернеті, використовуючи найбільш безпечний наразі механізм оплати.

Security Electronics Transaction – це протокол, призначений для забезпечення безпеки та цілісності електронних транзакцій, що здійснюються з використанням кредитних карток. На відміну від платіжної системи, SET працює як протокол безпеки, що застосовується до цих платежів. Він використовує різні методи шифрування та хешування для захисту платежів через Інтернет за допомогою кредитних карток.

Протокол SET обмежує розкриття даних кредитної картки продавцям, утримуючи таким чином хакерів і злодіїв. Протокол SET включає центри сертифікації для використання стандартних цифрових сертифікатів, таких як сертифікат X.509.

SET має наступні особливі **вимоги для захисту транзакцій** електронної торгівлі:

– Необхідно забезпечувати взаємну автентифікацію, тобто автентифікацію клієнта (або власника картки) шляхом підтвердження того, чи є клієнт цільовим користувачем, і автентифікацію продавця.

– Потрібно зберігати конфіденційність PI (Інформація про платіж) і OI (Інформація про замовлення) за допомогою відповідного шифрування.

– Обов'язкова стійкість до модифікації повідомлення, тобто не можна допускати жодних змін у вмісті, що передається.

– SET також має забезпечити взаємодію та використовувати найкращі механізми безпеки.

Учасники SET: у загальному сценарії онлайн-транзакцій SET включає схожих учасників:

1. Власник картки – клієнт

2. Емітент – фінансова установа-клієнт

3. Торговець

4. Еквайр – фінансовий торговець

5. Центр сертифікації – орган, який дотримується певних стандартів і видає сертифікати (наприклад, X.509V3) усім іншим учасникам.

Функціональність SET:

– **Проведення автентифікації**

– **Автентифікація продавця** – щоб запобігти крадіжці, SET дозволяє клієнтам перевіряти попередні відносини між продавцями та фінансовими установами. Для цієї перевірки використовуються стандартні сертифікати X.509V3.

– **Автентифікація клієнта/власника картки** – SET перевіряє, чи використовується кредитна картка авторизованим користувачем, чи не використовує сертифікати X.509V3.

– **Забезпечення конфіденційності повідомлень:** конфіденційність означає запобігання ненавмисним читанням повідомлення, що передається. SET забезпечує конфіденційність за допомогою методів шифрування. Традиційно DES використовується для цілей шифрування.

– **Забезпечення цілісності повідомлення:** SET не дозволяє модифікувати повідомлення за допомогою підписів. Повідомлення захищено від неавторизованої модифікації за допомогою цифрових підписів RSA з SHA-1, а деякі за допомогою HMAC з SHA-1,

Подвійний підпис – це концепція, представлена разом із SET, яка спрямована на з'єднання двох частин інформації, призначених для двох різних отримувачів.

Процес створення запиту на купівлю потребує трьох вхідних даних:

– Платіжна інформація (PI)

– Подвійний підпис

– Дайджест повідомлень з інформацією про замовлення (OIMD)

Заявка на купівлю формується таким чином, як показано на схемі. Тут:

– OI означає інформацію про замовлення;

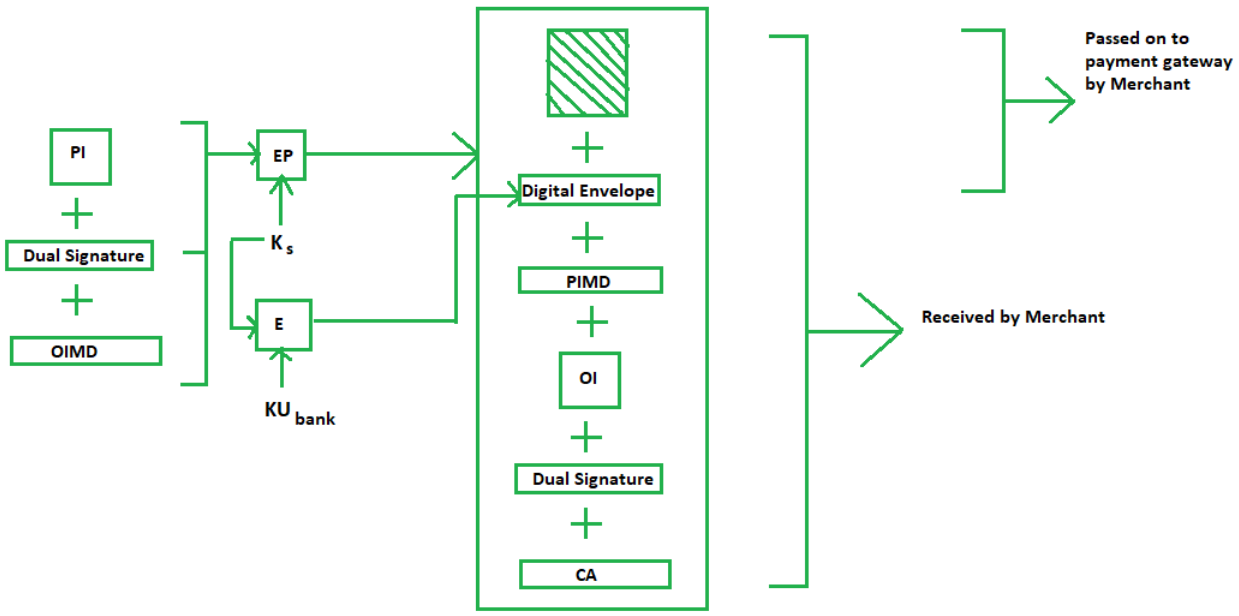
– EP – симетричний ключ шифрування;

– Ks – тимчасовий симетричний ключ;

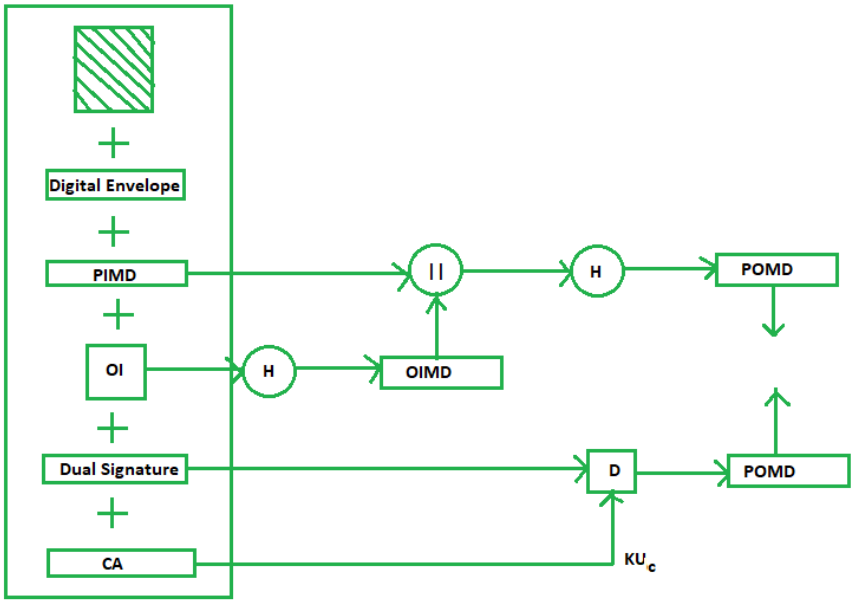
– KUbank – публічний ключ банку;

– CA – сертифікат власника картки або клієнта;

– Цифровий конверт = E(KUbank, Ks).



Продавець перевіряє, порівнюючи POMD (Payment Order Message Digest), згенерований за допомогою хешування PIMD (Payment Information Message Digest), із POMD (Payment Order Message Digest), згенерованим за допомогою розшифровки подвійного підпису таким чином як показано на наступній схемі:



Оскільки ми використовували приватний ключ клієнта для шифрування, ми тепер використовуємо KU_C, який є відкритим ключем клієнта або власника картки для розшифровки «D».

Властивості безпеки SET кращі, ніж SSL і більш сучасний TLS, особливо в їх здатності запобігати здирництву веббізнесу. Хай там що, найбільшим недоліком SET є його складність. SET вимагає від двох клієнтів і трейдерів запровадити екстраординарне програмування – перегляд карток і розширені гаманці – маючи на увазі, що учасникам біржі необхідно виконати більше завдань для виконання SET. Ця складність також знизила швидкість бізнес-обміну через Інтернет. SSL і TLS не мають таких проблем.

1.2 Безпека системи електронних платежів PayPal

Кожна транзакція, здійснена за допомогою PayPal, має ідентифікатор транзакції, рядок із 12 символів, за допомогою якого можна відстежувати статус або шукати транзакцію. Як зазначено на офіційному сайті, PayPal також надає такі послуги:

– підтвердження електронною поштою: ви отримуватимете електронний лист щоразу, коли надсилатимете чи отримуватимете платіж PayPal

– ключ безпеки PayPal: TLS 1.0 або вище

– HTTPS

– закріплення ключа

– шифрування даних

Ключ безпеки PayPal є другим фактором автентифікації на додачу до пароля. Він унікальний для кожного входу (одноразовий PIN-код – OTP). Кожного разу, коли ви захочете увійти, ви отримаєте код безпеки в SMS.

Методи шифрування даних:

1. Ви встановлюватимете підключення TLS щоразу, коли захочете отримати доступ до служби PayPal. PayPal переконається, що ви використовуєте TLS 1.0 або новішу версію та безпечне з'єднання (HTTPS).

2. Закріплення ключа: оскільки ви можете запустити програму PayPal на своєму мобільному телефоні, а зловмисник видає себе за справжній сервер PayPal, перехоплюючи запит, PayPal гарантує, що ви підключаєтеся до справжнього сервера PayPal, коли встановлено з'єднання TLS.

PayPal відповідає PCI-DSS. Payment Card Industry (PCI) Data Security Standard (DSS), PCI-DSS — це стандарт, якого всі організації, включно з роздрібними торговцями в Інтернеті, повинні дотримуватися ряду вимог як передової практики. Компанія повинна використовувати брандмауер між бездротовою мережею та середовищем даних власника картки, використовувати найновіші засоби безпеки та автентифікації, такі як WPA/WPA2, а також змінити параметри за замовчуванням для дротових ключів конфіденційності та використовувати систему виявлення мережевого вторгнення, щоб бути сумісною з PCI.

Стандарт безпеки даних рекомендує потрійне шифрування даних (Triple DES) для PIN-шифрування. Потрійний DES — це алгоритм блокового шифрування, у якому кожен блок містить 64 біти даних і 56 бітів для кожного ключа. У Triple DES ключі ідентичні. Потрійний DES є кращим рішенням, замінюючи DES як стандарт PIN-шифрування. TDES надає такі переваги:

1. Краща безпека електронних платежів завдяки доданим рівням безпеки та потрійному запуску алгоритму шифрування. Це важче зламати та/або пошкодити.

2. Проста система з одним алгоритмом.

3. Відповідність потрійному шифруванню даних продавцями, які хочуть полегшити дебетові операції з PIN-кодом, є обов'язковою через підвищену безпеку, яку вона забезпечує.

4. Кращий сервіс і безперебійна робота, без атак і вторгнень.

Безпека блокового шифру часто зводиться до розміру блоку цього шифру. Через короткий розмір блоку в 64 біти Triple DES вразливий до атаки колізії блоків.

Атака Sweet32 демонструє наскільки Triple DES вразливий до атак днів

народження. Для атаки Triple DES в TLS потрібно 785 GB блоків (близько 2^{36}), але дослідники отримали колізію після 2^{30} блоків.

Стандарти безпеки PCI також рекомендують використовувати похідний унікальний ключ для кожної транзакції. Це метод керування ключами, який використовує унікальний ключ для кожної транзакції та запобігає розголошенню будь-якого минулого використаного ключа. Унікальні ключі транзакцій виводяться з базового ключа деривації з використанням лише несекретних даних, що передаються як частина кожної транзакції.

На офіційному вебсайті PayPal вказана вся інформація, яку PayPal збирає:

– інформація про реєстрацію та використання;

– інформація про транзакції та досвід: інформація про трансакції; надіслана чи запитана сума; сума, сплачена за продукти чи послуги; інформація про продавця, включаючи інформацію про будь-які інструменти фінансування, використані для завершення транзакції; інформація про пристрій; технічні дані про використання та інформація про геолокацію;

– інформація про учасника;

– інформація про друзів і контакти;

– інформація, яку вибрано для надання про отримання додаткових послуг або конкретних онлайн-послуг;

– інформація про вас, якщо ви здійснюєте транзакцію як гість;

– інформація про вас зі сторонніх джерел.

ВИСНОВКИ

SET - це стандарт, який дозволяє користувачам купувати товари в Інтернеті, використовуючи найбільш безпечний наразі механізм оплати.

SET дозволяє сторонам ідентифікувати себе одна перед одною та безпечно обмінюватися інформацією. Прив'язка ідентичностей ґрунтується на сертифікаті X.509 із кількома розширеннями. SET використовує криптографічний алгоритм засліплення, який, по суті, дозволяє продавцям замінити номер кредитної картки користувача сертифікатом. Якби всюди використовувався SET, самому продавцю ніколи б не довелося знати номери кредитних карток, надісланих від покупця, що забезпечило б підтверджену належну оплату, але захистило клієнтів і кредитні компанії від шахрайства.

SET мав стати де-факто стандартним методом оплати в Інтернеті між продавцями, покупцями та компаніями, що видають кредитні картки.

На жаль, впровадження кожною з основних зацікавлених сторін було або дорогим, або громіздким. Були також деякі зовнішні фактори, які могли ускладнити інтеграцію елемента споживача в браузер, тому цей протокол запроваджений не всюди.

Один з основних протоколів, що використовується в системі PayPal, – це протокол TLS. Він забезпечує шифрування даних, що передаються між клієнтом та сервером, та автентифікацію сервера. Крім того, система PayPal використовує інші криптографічні протоколи, такі як Triple DES, для забезпечення безпеки та захисту даних.