ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ
УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

Лабораторна робота №6

з курсу «Безпека банківських систем»

ВИВЧЕННЯ ЗАХИСТУ ПОВІДОМЛЕНЬ В ПРОТОКОЛІ SET

Харків 2023

Мета: ознайомитися з принципами роботи протоколу SET (Secure Electronic Transaction).

1 ТЕОРЕТИЧНІ ВІДОМОСТІ

1.1 Можливості протоколу SET щодо захисту транзакцій в інтернет

Протокол SET (Secure Electronic Transaction – протокол захищених електронних транзакцій) являє собою відкриті специфікації, розроблені з метою захисту транзакцій, в Internet за допомогою пластикових платіжних карток.

SET є набором протоколів захисту і форматів даних, що дозволяють захищеним чином використовувати наявну інфраструктуру платіжних систем пластикових карток у відкритих мережах типу Internet. По суті, SET забезпечує наступні три види сервісу:

1. Створення захищеного комунікаційного каналу, який зв'язує всі сторони, що беруть участь у транзакції.

2. Забезпечення довіри за допомогою цифрових сертифікатів X509v3.

3. Забезпечення таємності через те, що інформація виявляється доступною тільки учасникам транзакції і тільки тоді і там, де вона необхідна.

У протоколі SET реалізовані такі можливості:

– конфіденційність інформації. Інформація про рахунок власника карти і платежі захищається під час пересилання по мережі. Цікава і важлива особливість SET полягає в тому, що продавець при цьому не може з'ясувати номер кредитної картки її власника – ця інформація виявляється доступною тільки банку, який видав кредитну картку. Для забезпечення конфіденційності використовується шифрування за традиційною схемою за допомогою симетричного алгоритму DES (Data Encryption Standard) а також за допомогою несиметричного алгоритму RSA (абревіатура від прізвищ Rivest, Shamir та Adleman);

– цілісність даних. Інформація про платіж, що посилається власником карти продавцю, містить інформацію про замовлення, особисті дані й інструкції для здійснення платежу. SET гарантує, що зміст відповідних повідомлень не буде змінено під час їх передачі. Цілісність даних досягається за допомогою цифрових підписів RSA, що використовують хеш-коди SHA-1 (Secure Hash Algorithm 1);

– автентифікація рахунка власника карти. SET дає продавцю можливість перевірити, чи є пред'явник кредитної картки законним користувачем відповідного дійсного рахунка. Для цієї мети в SET передбачене використання цифрових сертифікатів X.509v3 з підписами RSA;

– автентифікація продавця. SET дозволяє власнику карти перевірити, чи має продавець відношення до відповідної фінансової організації і право приймати платежі по кредитних картках. Для цієї мети в SET передбачене використання цифрових сертифікатів X.509v3 з підписами RSA.

Зверніть увагу на те, що на відміну від IPSec і SSL/TLS протокол SET для вирішення кожної конкретної задачі пропонує тільки по одному алгоритму. Це пояснюється тим, що SET є протоколом, що відповідає цілком конкретному набору вимог, тоді як IPSec і SSL/TLS відносяться до універсальних протоколів, призначених для вирішення широкого спектра задач.

1.2 Учасники транзакцій SET

Учасниками транзакцій, здійснюваних за допомогою SET, є такі сторони (рис. 1).

Власник платіжної карти. У середовищі електронних платежів індивідуальні і корпоративні споживачі взаємодіють із продавцями зі своїх персональних комп'ютерів через Internet. Власником карти в даному випадку є будь-якийзареєстрований власник пластикової платіжної карти (MasterCard, Visa і т.п.), виданої йому уповноваженим емітентом.

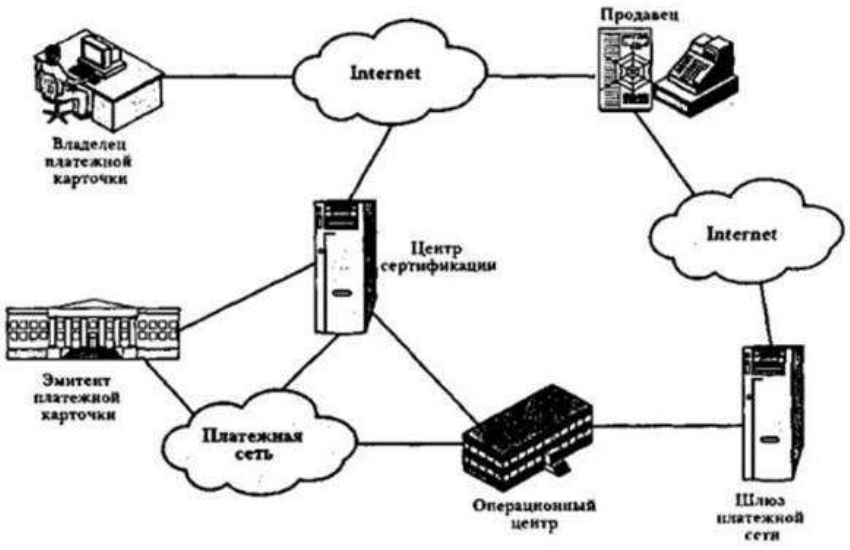


Рис. 1. – Учасники та компоненти захищеної системи електронної комерції.

Продавець. Продавець є особою, у якої власник карти може придбати товари чи послуги. Звичайно такі товари чи послуги пропонуються на продаж на Web-вузлі чи по електронній пошті. Продавець, що має право приймати платежі по платіжних картах, повинен мати відповідні відносини з операційним центром.

Емітент платіжної картки. Емітент – це фінансова організація (наприклад банк), що видала платіжну карту відповідній особі (власнику карти). Як правило, відкрити рахунок можна дистанційно чи в офісі емітента особисто. Усю відповідальність по оплаті заборгованості власника карти по даній карті несе емітент.

Операційний центр. Фінансова організація, що веде розрахунки з продавцем та виконує авторизацію платіжних карт і здійснює відповідні платежі. Операційний центр проводить для продавця перевірку того, що рахунок кредитної карти є дійсним, і пропонована покупка по вартості не виходить за рамки припустимого кредитного ліміту. Операційний центр також виконує електронний переказ грошових сум на рахунок продавця. Згодом операційний центр одержує за це визначену компенсацію від емітента карти через банківську платіжну мережу.

Шлюз платіжної мережі (payment gateway). Сукупність засобів, контрольованих операційним центром чи уповноваженою ним третьою стороною, що використовуються для обробки платіжних повідомлень продавця. Шлюз платіжної мережі зв'язує SET і банківські платіжні мережі, виконуючи функції авторизації та передачі платежів. Продавець обмінюється повідомленнями SET зі шлюзом платіжної мережі через Internet, а шлюз платіжної мережі зв'язаний безпосередньо чи по внутрішній мережі із системою обробки фінансових документів відповідного операційного центра.

Центр сертифікації (Certification Authority – CA). Об'єкт, якому довіряється видавати сертифікати X.509v3 відкритихключів власників карт, продавців і шлюзів платіжної мережі. Успішна робота SET багато в чому залежить від наявності добре організованої інфраструктури сертифікації.

Тепер опишемо коротко послідовність подій, що відбуваються під час транзакції, а потім зупинимося докладніше на деяких криптографічних деталях даного процесу.

1. Покупець відкриває рахунок. Покупець відкриває рахунок кредитної картки (наприклад, MasterCard чи Visa) у банку, що здійснює електронні платежі і підтримує SET.

2. Покупець одержує сертифікат. Після встановленої процедури перевірки особистості покупець одержує цифрові сертифікати X.509v3, підписані центром сертифікації. Один з сертифікатів засвідчує відкритий ключ цифрового підпису, другий – відкритий ключ направленого шифрування. Ці сертифікати засвідчують відкриті RSA ключі покупця і їх термін дії. Вони також установлюють відповідність між парою ключів покупця і його кредитною карткою.

3. Продавець одержує свої сертифікати. Продавець, який хоче приймати оплату по платіжній картці визначеного типу, повинен одержати два сертифікати двох своїх відкритих ключів: один з них буде використовуватися для цифрового підпису, а другий – для направленого шифрування. Продавцю

також буде потрібна копія сертифіката відкритого ключа шлюзу платіжної мережі.

4. Покупець розміщує замовлення. Цей процес може припускати, що покупець спочатку повинен відвідати Web-вузол продавця, щоб вибрати потрібний товар і визначити ціну. Після цього покупець відправляє продавцю список потрібних йому товарів, а продавець у відповідь висилає бланк замовлення з зазначеними в ньому списком обраних товарів, цінами, загальною вартістю замовлення і номером замовлення.

5. Перевірка продавця. Разом із бланком замовлення продавець висилає копію свого сертифіката, щоб покупець мав можливість переконатися в тому, що він дійсно має справу зі справжнім продавцем.

6. Замовлення і платіж відправляються продавцю. Покупець відправляє замовлення і платіжну інформацію продавцю, додаючи до них свій сертифікат. Замовлення підтверджує покупку товарів, зазначених у бланку замовлення. Платіжна інформація містить необхідні дані кредитної картки. Платіжна інформація шифрується таким чином, щоб продавець не зміг її прочитати. Сертифікат покупця дозволяє продавцю виконати верифікацію покупця.

7. Продавець запитує авторизацію платежу. Продавець відправляє платіжну інформацію шлюзу платіжної мережі з запитом підтвердження того, що доступний покупцю кредит достатній для здійснення даного платежу.

8. Продавець підтверджує замовлення. Продавець відправляє покупцю підтвердження замовлення.

9. Продавець доставляє товари чи надає послуги.

10. Продавець запитує одержання платежу. Цей запит відправляється шлюзу платіжної мережі, що опрацьовує всі платіжні доручення.

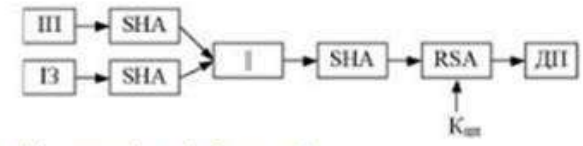
1.3 Дуальний підпис

Розглянемо одне важливе нововведення SET – дуальний підпис (dual signature). Дуальний підпис дозволяє зв'язати два повідомлення, призначені двом різним одержувачам. У даному випадку покупцю потрібно переслати

інформацію про замовлення (ІЗ) продавцю і платіжну інформацію (ІП) банку. Продавцю не потрібно знати номер кредитної картки покупця, а банку не потрібні подробиці замовлення. Покупець же, розділяючи ці повідомлення, забезпечує тим самим додатковий захист своїх прав з погляду невтручання в його особисте життя. При цьому потрібно зв'язати ці повідомлення так, щоб їх можна було використовувати при виникненні конфлікту. Зв'язок цих частин потрібен для того, щоб покупець міг довести, що даний платіж призначений для оплати саме цього, а не якогось іншого замовлення.

Щоб зрозуміти необхідність такого зв'язку, припустимо, що покупець відправляє продавцю два підписаних повідомлення ІЗ (замовлення) і ІП (платіж), а продавець пересилає повідомлення ІП у банк. Якщо продавець одержить від покупця якесь інше замовлення, то продавець зможе заявити, що дане повідомлення ІП оплачує нове, а не старе повідомлення ІЗ. Зв'язування виключає таку можливість.

На рис. 2 показана схема використання дуального підпису: спочатку покупець, використовуючи алгоритм SHA-1, обчислює хеш-коди для повідомлень ІП і ІЗ. Два отриманих хеш-коди зв'язуються операцією конкатенації, і для результату зв'язування теж обчислюється хеш-код. Нарешті, покупець шифрує підсумковий хеш-код з використанням свого особистого ключа цифрового підпису, у результаті одержуючи дуальний підпис.



ІП — платіжна інформація

ІЗ — інформація про замовлення

SHA — функція хешування (SHA-1)

|| — конкатенація

RSA — шифрування (RSA)

КЦП — особистий ключ підпису покупця

ДП – дуальний підпис

Рис. 2. – Створення дуального підпису

1.4 Реалізація транзакцій у протоколі SET

Опишемо тепер типи транзакцій, які є у протоколі SET. У протоколі SET повідомлення, за допомогою яких реалізуються різні транзакції, мають парний характер (запит-відповідь), *Payment Initialization Request/Response Messages*. Ця пара повідомлень використовується для взаємної аутентифікації власника картки та торгової точки, для передачі власнику картки від торгової точки необхідних сертифікатів та списків CRL, а також надання інформації торгової точки про те, яка картка платіжної системи буде використовуватися при проведенні покупки.

Purchase Order Request/Response Messages. Ця пара повідомлень служить для передачі в захищеній сесії від власника картки до торгової точки інформації про замовлення (сума купівлі, валюта, номер торгової точки тощо) та реквізити картки власника картки.

Authorization Request/Response Messages. Запит *AuthorizationRequest* ініціюється торговою точкою та передається платіжному шлюзу для передачі йому даних щодо транзакції та реквізитів картки. Надалі ці дані будуть використані для формування повідомлення, яке передається емітенту картки через платіжну мережу.

Gateway Certificate Request/Response Messages. Ця пара повідомлень дозволяє торговій точці запросити у платіжного шлюзу його сертифікат *Key-Exchange Key*.

Batch Administration Request/Response Messages. Ця пара повідомлень використовується для адміністрування наборів (batch) транзакцій для того, щоб торгова точка та обслуговуючий банк могли провести звіряння даних кожної сторони. Запит дозволяє відкривати нові набори транзакцій, відкривати та закривати існуючі набори транзакцій, а також з'ясовувати їхній статус.

Inquiry Request/Response Messages. За допомогою цієї пари повідомлень власник картки може з'ясувати статус виконання електронної покупки (отримано позитивну авторизацію, зроблено замовлення, у процесі доставки,

товар доставлено тощо). *InquiryRequest* може бути відправлений власником картки у будь-який час та будь-яку кількість разів.

Authorization Reversal Request/Response Messages. Пара повідомлень використовується для того, щоб скасувати раніше проведену авторизацію. Ця пара повідомлень може також використовуватися для того, щоб скоригувати розмір транзакції раніше виконаної авторизації.

Capture Request/Response Messages. Повідомлення *Capture Request* передається від торгової точки до платіжного шлюзу і просить у обслуговуючого банку платіж за зроблену покупку. Розмір запитуваного платежу має бути раніше авторизований банком-емітентом власника картки за допомогою повідомлень *Authorization Request/Response*. Зазвичай торгова точка ініціює запит *Capture Request* після виконання замовлення, пов'язаного з електронною покупкою.

Credit Request/Response Messages. Ця пара використовується для того, щоб повернути раніше зроблений платіж обслуговуючого банку на адресу торгової точки.

Credit Reversal/Response Messages. Ця пара повідомлень дозволяє торговій точці скасувати кредит на користь обслуговуючого банку.

Розглянемо тепер докладніше, як реалізується операція електронної купівлі з допомогою протоколу SET.

Власник картки ініціює покупку за допомогою повідомлення *PinitReq*. У цьому повідомленні власник картки передає торговій точці сформований ним ідентифікатор парою повідомлень *PinitReq/PinitRes*, ідентифікатор транзакції LID-C, згенерований власником картки для обліку в системі власника картки, ідентифікатор платіжної системи Brand ID, карткою якої власник картки (перші 6 цифр номера картки) розраховується, мова, що використовується власником картки для здійснення операції, параметричні «відбитки» сертифікатів, списків CRL та каталогу BCI, що зберігаються в системі власника картки, випадкове число Chall-C, згенероване власником картки, параметричний ідентифікатор транзакції в системі торгової точки.

У відповідному повідомленні *PinitRes* торгова точка формує такі дані:

– копіює із запиту власника картки дані LID-C та мову;

– генерує глобальний ідентифікатор транзакції XID;

– копіює із запиту *PinitReq* «відбитки» сертифікатів, списки відкликаних сертифікатів, каталоги BCI, Chall-C;

– генерує випадкове число Chall-M;

– на підставі Brand ID, BIN та сертифіката власника картки вибирає відповідний платіжний шлюз та вставляє у повідомлення сертифікат *Key-Exchange Key* цього платіжного шлюзу;

– вставляє у повідомлення поточний каталог BCI, якщо у запиті клієнта «відбиток» каталогу BCI був відсутній або був присутній «відбиток» вже неактуального каталогу (нагадаємо, що відповідно до прийнятих у протоколі SET угоди поряд з BCI у полі CRL даних *SignedData* передаються також асоційовані з даними BCI списки CRL);

– деякі інші дані.

Торгова точка підписує дані своїм закритим ключем *Signing Key* і спрямовує сформоване таким чином повідомлення власнику картки.

Інші етапи реалізації електронної купівлі будуть описані менш детально.

Власник картки перевіряє отримані сертифікати відкритого ключа підпису торгової точки та відкритого ключа *Key-Exchange Key* платіжного шлюзу, після чого перевіряється цифровий підпис торгової точки в отриманому повідомленні. Таким чином, власник картки автентифікує торгову точку.

Після цього власник картки починає формування повідомлення *PReq*. Це повідомлення складається з двох частин: інструкції на замовлення (*Order Instruction, OI*) та платіжної інструкції (*Payment Instruction, PI*).

OI призначено для торгової точки і включає значення Chall-M з повідомлення *PinitRes*, ідентифікатор транзакції XID, розмір транзакції і валюту транзакції, ідентифікатор торгової точки, ідентифікатор *batch*, до якого повинна бути віднесена покупка, номер замовлення в системі магазину, хеш-

функцію від PI та деяку іншу інформацію. PI призначено для платіжного шлюзу і включає ідентифікатор транзакції XID, величину *TranStain*, що представляє собою хеш-функцію від секрету карти S і XID, хеш-функцію OI, параметричне значення CVC2/CVC2, 2-у доріжку магнітної смуги карти та іншу інформацію.

Далі власник карти обчислює хеш-функцію від послідовності, що складається зі значень хеш-функції від PI та OI, і підписує отримане значення своїм секретним ключем.

Власник карти генерує випадково симетричний ключ K1, за допомогою якого він шифрує PI. Значення ключа K1 разом із даними по карті (номер картки, термін її дії та секрет карти), у свою чергу, закриваються за допомогою відкритого ключа *Key-Exchange Key* платіжного шлюзу. Повідомлення *Preq* складається з OI, зашифрованої інструкції PI, зашифрованих даних про реквізити карти та ключа K1, цифрового підпису власника картки.

Торгова точка, отримавши повідомлення *PReq*, перевіряє сертифікат власника картки, після чого перевіряє цифровий підпис власника картки. Для перевірки цифрового підпису торгова точка обчислює значення хеш-функції від OI і далі, використовуючи значення хеш-функції для PI , обчислює загальне значення H. Після цього за допомогою відкритого ключа власника карти дешифрується отримане з *PReq* повідомлення цифрового підпису. Якщо дешифроване значення збігається із загальним значенням, підпис був зроблений власником сертифіката відкритого ключа власника картки. Таким чином: торгова точка автентифікує власника картки.

Далі торгова точка готує повідомлення *AuthReq*. До цього повідомлення без змін включено із повідомлення *PReq* зашифровану платіжну інструкцію PI, зашифрований симетричний ключ K1 та дані про реквізити картки, а також цифровий підпис власника картки. Крім цих даних, торгова точка формує авторизаційний запит, що містить інформацію про розмір транзакції, ідентифікатор торгової точки, ідентифікатор транзакції XID, випадкове число *Chall-P* та інше. Ця інформація підписується ключем *Signing Key* торгової

точки, закривається симетричним ключем К2 згенерованим торговою точкою за випадковим законом, який закривається відкритим ключем *Key-Exchange Key* платіжного шлюзу.

Платіжний шлюз, отримавши *AuthReq*, дешифрує за допомогою закритого ключа *Key-Exchange Key* обидва симетричні ключі К1 і К2, а також дані про реквізити карти, дешифрує дані про транзакцію та PI, перевіряє підпис власника картки (за аналогією з тим, як це робить торгова точка, для цього використовується значення Н, що міститься в PI), перевіряє на рівність значення XID з інформації про транзакцію та PI. Таким чином, платіжний шлюз автентифікує як торговельну точку, так і власника картки. На основі отриманих даних платіжний шлюз готує стандартне повідомлення (наприклад, у форматі ISO 8583) для передачі його до платіжної системи на авторизацію емітента картки.

Отримавши з платіжної системи відповідь, платіжний шлюз генерує і підписує своїм закритим *Signing Key* повідомлення *AuthRes* (у повідомленні міститься випадкова величина *Chall-P*, також дані *Capture Token*, в яких платіжний шлюз запитує у торгової точки очікувані дані від торгової точки в повідомленні *Capture Request*). Повідомлення зашифровується за допомогою згенерованого для цього симетричного ключа, який закривається за допомогою відкритого ключа торгової точки.

Торгова точка дешифрує симетричний ключ, перевіряє цифровий підпис платіжного шлюзу та формує повідомлення *PRes*, що містить *Chall-C*, підписуючи його своїм закритим *Signing Key*.

Власник картки, отримавши повідомлення *PRes*, перевіряє цифровий підпис торгової точки. У цьому процес електронної купівлі може бути завершено.

Розрахунки між торговою точкою та обслуговуючим банком здійснюються або на підставі наведеної раніше схеми електронної купівлі, або на підставі додаткового запиту *Capture Request* від торгової точки.

3 ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

1. Виконати дослідження методів шифрування, що використані в протоколі SET (DES та RSA).

2. Розробити програму шифрування повідомлень з використанням або симетричного алгоритму DES, або за допомогою несиметричного алгоритму RSA.

3. В якості мови програмування використати будь-яку мову на ваш вибір.

4. Навести вихідний код програми.

5. Разом зі звітом надати скомпільовану програму у архіві.

Запитання для самоперевірки

1. Що таке протокол SET?

2. Для чого використовується протокол SET?

3. Які засоби шифрування в ньому використовуються?

4. Чим гарантується цілісність даних в протоколі SET?

5. За рахунок чого відбувається автентифікація рахунка власника карти в протоколі SET?