ДИПЛОМНА РОБОТА

ДОСЛІДЖЕННЯ ТА ПРОЕКТУВАННЯ MONDEX СЕРЕДОВИЩЕ

Виконав: студент 641 н/г Жук Б. Ю.

Керівник практики: Крюковский Р. І.

Розробка програмного забезпечення (м. Васильків)

Актуальність вибраної теми

Необхідність здійснювати грошові перекази і комерційні платежі виникла давно, але з появою інтернету, з'явилася і така дуже зручна і необхідна послуга як інтернет-платежі. У сучасному світі простежується чітка тенденція розвитку, і широке поширення платіжних систем. З кожним роком підвищується актуальність електронних грошей. Операціями з оплати комунальних платежів і грошовими переказами займаються і онлайн-банки (наприклад, ПриватБанк), і такі послуги з кожним роком мають більший попит.

Мета та задачі роботи

Мета дипломної роботи полягає в дослідженні розвитку платіжної системи Mondex. Для досягнення мети були посалені наступні завдання :

– Структура платіжної системи Mondex;

– Класифікація платіжних систем;

– Основи функціонування платіжних систем;

Об'єкт та предмет дослідження

Об'єктом дослідження є робота та функції платіжної системи Mondex.

Предмет дослідження – стратегії розвитку електронної платіжної системи Mondex.

Методи дослідження – узагальнення та систематизація платіжної системи тощо.

Що таке платіжна система?

Платіжна система - система розрахунків між фінансовими організаціями (комерційними банками, небанківськими кредитними організаціями, інвестиційними організаціями), бізнес-організаціями та інтернет-користувачами при покупці-продажу товарів і за надання різних послуг через інтернет. Платіжна система є різновидом традиційних платіжних систем і

за схемою оплати поділяються на: дебетові (працюючі з електронними чеками і цифровою готівкою); кредитні (які працюють з кредитними картками).

Види платіжних систем

- **Внутрішньодержавна платіжна система** — платіжна система, в якій платіжна організація є резидентом та яка здійснює свою діяльність і забезпечує проведення переказу коштів винятково в межах України.

- **Міждержавні платіжні системи**

Завдання і функції платіжних систем

Основними завданнями, що стоять перед платіжною системою, є наступні:

- безперебійність, безпеку і ефективність функціонування;
- надійність і міцність, що гарантують відсутність зривів або повного виходу з ладу системи платежів;
- ефективність, що забезпечує швидкий,
- економний і точний вихід потоку операцій;
- справедливий підхід, наприклад вимога участі в платіжній системі осіб, що відповідають необхідним кваліфікаційним критеріям.

Основною функцією будь-якої платіжної системи є забезпечення динаміки і стійкості господарського обороту.

Елементи платіжної системи

Елементи платіжної системи тісно взаємопов'язані між собою, їх взаємодія здійснюється за певними правилами, закріпленим в нормативно-правових актах (НПА) держави і міжнародних угодах.

До **елементів платіжної системи** належать такі:

- **інститути**, що надають послуги із здійснення грошових переказів і погашення боргових зобов'язань;
- **фінансові інструменти** та комунікаційні системи, забезпечують переказ грошових коштів між економічними агентами;
- **контрактні угоди**, що регулюють порядок безготівкових розрахунків.

Покупки за допомогою Mondex

Щоб здійснити платіж, досить вставити картку Мондекс в щілину зчитувача карток роздрібного терміналу. Необхідна сума відразу ж переводиться з картки на термінал, причому не потрібні ні підпису, ні авторизація.

Продавці газет і дрібні торговці можуть використовувати термінали на батарейках.

Поповнення та зчитування залишку на картці

Картку можна перезавантажити електронними грошима на спеціально пристосованих **пристроях для видачі грошей** або - по **телефону**.

У найближчі десять років телефон, мабуть, стане **основним засобом для внесення депозитів** в банки і для їх вилучення. Мобільні телефони, сумісні з системою Мондекс, будуть здатні виконувати функції як Ваш власний мобільний розподільник грошей. Спеціально пристосовані таксофони також здатні здійснювати переказ грошових коштів.

Платежі по мережі Інтернет

Електронні готівкові гроші можуть переноситися з картки на картку за допомогою портмоне системи Мондекс настільки ж просто, як просто передати фізичні гроші від однієї особи іншій. Батьки зможуть використовувати це портмоне, щоб дати електронні кишенькові гроші своїм дітям. Портмоне дозволяє також бачити деталі Ваших останніх десяти транзакцій, так що Ви можете бачити, куди в кінцевому підсумку йдуть Ваші гроші.

Безпека та надійність

Мондекс не розкриває деталей роботи своєї системи, перш за все щодо криптографічного захисту, відкритих шифроключей і використовуваних алгоритмів. Кожен електронний гаманець отримує свій 16-ти розрядний унікальний ідентифікаційний номер, який ототожнюється з його власником.

Активація електронного гаманця Мондекс відбувається тільки після введення довільного індивідуального 4х-значного PIN-коду безпосередньо конкретним користувачем. Невдалі 3х-разові спроби підібрати PIN-код призводять до "закриття" електронного гаманця Мондекс.

Мондекс використовує електронний підпис для впізнання справжності карток і виявлення спроб шахрайства.

Структура платіжної системи

Система Mondex складається з ієрархічної структури класу гаманця, що складається з чотирьох різних варіантів смарт-карт Mondex, які здатні приймати, зберігати та розподіляти гроші. Фінансові установи, споживачі та торговці мають різні класи карт. Це зроблено з міркувань безпеки. По-перше, тому що всі учасники тримають картки, система може бути спроектована як абсолютно замкнута: тільки Орієнтифікатор може замалювати або знищити значення Mondex.

Структура зв'язку Mondex

Як картка із збереженим значенням із сильним шифруванням, Mondex працює поза мережею без сторонньої клірингової системи. Кожна передача відбувається безпосередньо між залученими сторонами та ізольована від усіх інших переказів. Оскільки всі комунікації між читачами зашифровані, Mondex може використовувати відкриті мережі зв'язку, такі як телефонна система або Інтернет. Картрідери можуть бути приєднані до комп'ютерів або телефонів - як існуючі читачі телефонних карт - і їх також можна використовувати, наприклад, в магазинах, автобусах або паркувальних лічильниках. Однак ця процедура призводить до суттєвого посилення ризиків безпеки. Якщо карта може бути підроблена та введено нові гроші в систему, було б неможливо диференціювати підроблені з законних грошей.

Безпека

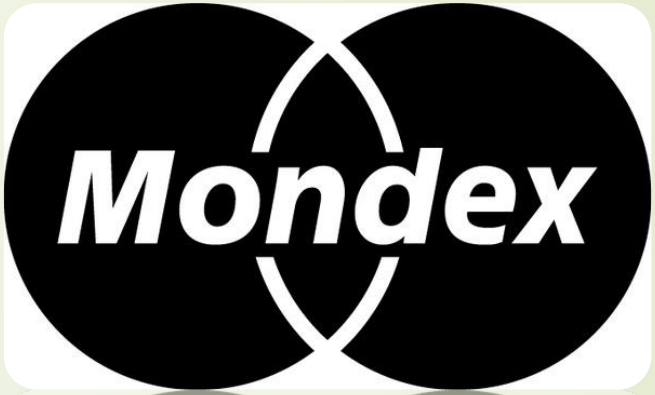
Якщо можна було ввести несанкціоновані гроші в обіг, ці гроші не можна розрізнити з законних грошей, оскільки гроші фактично створюються з кожною операцією. Щоб відповідати високим стандартам, концепція безпеки Mondex складається з трьох елементів: ***попередження***, ***виявлення*** та ***відновлення***.

Виявлення - Коли карта Mondex зв'язується з фінансовою установою, збираються статистичні дані, на яких, згідно з Mondex, можна провести комплексний аналіз поведінки використання картки.

Відновлення - Mondex гарантує, що "картки, які ідентифікуються як несанкціоновані, повідомлені вкрадені або потенційно шахрайські, можуть бути відключені безпосередньо від банківської системи".

Профілактика - Стратегія профілактики складається з декількох етапів: вона починається з двох основних елементів у системі Mondex - апаратної частини чіпа, вбудованого в карту, та програмного забезпечення, яке контролює рух вартості між картками.

Параметри



Mondex надає технічно передові рішення для широкого спектра платіжних ситуацій, і в кінцевому підсумку може сполучити традиційні з новою
електронною комерцією, що потенційно стимулює розвиток обох. Його однорангові та офлайн-функції дозволяють розширити децентралізовані, неформальні та відносно приватні особливості традиційних грошових коштів у електронних засобах масової інформації. Однак, як і багато хто з його конкурентів, Mondex має проблемні аспекти. Вони відображають небезпеку нерівномірно розвивається інформаційного суспільства: по-перше, виключення тих, хто має незначну економічну цінність як споживачів, і, по-друге, виникнення потужних приватних інститутів, які працюють поза межами, встановленими традиційними демократичними інститутами.

ВИСНОВКИ

У дипломній роботі виконанні дослідження що спрямовані на підвищення швидкості захисту електронних інформаційних ресурсів за рахунок використання запропонованої системи контролю цілісності.

У процесі виконання роботи отримані такі результати:

1. Проаналізовано сучасні системи криптозахисту даних, що дозволило вивчити їх структуру для можливого використання при удосконаленні алгоритму MD5.
2. Проведено дослідження існуючих алгоритмів хешування, що дозволило побудувати методику удосконалення хеш-функції MD5.
3. Удосконалено алгоритм хешування MD5 за рахунок зменшення кількості операцій та зміни самих операцій, що дало можливість підвищити його швидкодію на 20%.
4. Розроблено алгоритм та ПЗ удосконаленої системи контролю цілісності державних інформаційних ресурсів, які можуть бути використані для захисту електронних інформаційних ресурсів, та дозволили провести верифікацію удосконаленого методу контролю цілісності.

Дякую за увагу!