Безпека мікропроцесорних карток

Лектор:
Лимаренко Вячеслав Володимирович
к.т. 066-070-8586

Види платіжних карток, основні поняття

Пластикова картка – це персоніфікований платіжний інструмент, що надає особі, яка користується карткою, можливість безготівкової оплати товарів і/або послуг, а також одержання готівки у відділеннях (філіях) банків і банківських автоматах (банкоматах).

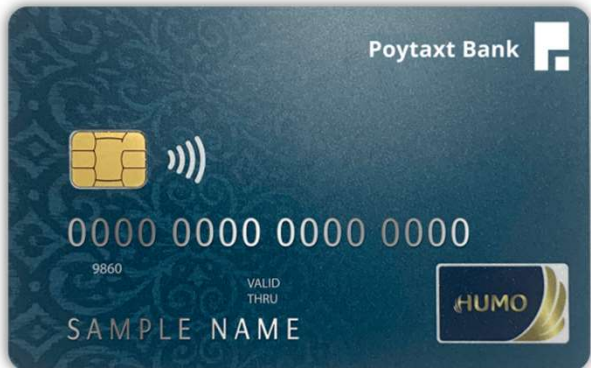
Підприємства торгівлі/сервісу і відділення банків, що приймають картку, утворюють мережу точок обслуговування картки (або приймальну мережу).

Особливістю продажів і видачі готівки за картками є те, що ці операції здійснюються магазинами і, відповідно, банками «у борг» – товари і готівка надаються клієнтам відразу, а кошти в їхнє відшкодування надходять на рахунки обслуговуючих підприємств найчастіше через якийсь час (не більше кількох днів).

Види платіжних карток, основні поняття

Гарантом виконання платіжних забов'язань, що виникають у процесі обслуговування пластикових карток, є банк-емітент, що їх випустив. Тому картки протягом усього терміну дії *залишаються власністю банку*, а клієнти, які мають картку, одержують їх лише в користування. Характер гарантій банку-емітента залежить від платіжних повноважень, наданих клієнту, і класу картки.

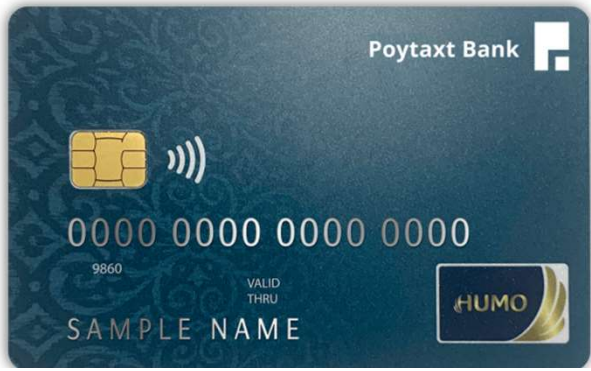
При видачі картки клієнту здійснюється її *персоналізація* – на неї заносяться дані, що дають змогу ідентифікувати картку та її власника, а також перевірити платоспроможність картки при прийомі її до оплати чи видачі готівки.



Види платіжних карток, основні поняття

Гарантом виконання платіжних забов'язань, що виникають у процесі обслуговування пластикових карток, є банк-емітент, що їх випустив. Тому картки протягом усього терміну дії *залишаються власністю банку*, а клієнти, які мають картку, одержують їх лише в користування. Характер гарантій банку-емітента залежить від платіжних повноважень, наданих клієнту, і класу картки.

При видачі картки клієнту здійснюється її *персоналізація* – на неї заносяться дані, що дають змогу ідентифікувати картку та її власника, а також перевірити платоспроможність картки при прийомі її до оплати чи видачі готівки.



Види платіжних карток, основні поняття

Процес затвердження продажу чи видачі готівки за карткою називається *авторизацією*. Для її здійснення точка обслуговування робить запит платіжній системі про підтвердження повноважень пред'явника картки і його фінансових можливостей.

Технологія авторизації залежить від схеми платіжної системи, типу картки і технічного оснащення точки обслуговування. *Авторизація* здійснюється «вручну», коли продавець чи касир телефонує оператору (голосова авторизація), або автоматично, при цьому картку поміщають у POS-термінал або торговий термінал, дані зчитуються з картки, касир вводить суму платежу, а власник картки зі спеціальної клавіатури – секретний *ПІН-код* (PIN-код). Після цього термінал здійснює авторизацію або за допомогою встановлення зв'язку з базою даних платіжної системи (online режим), або у результаті додаткового обміну даними із самою карткою (offline авторизація). У разі видачі готівки процедура має аналогічний характер з тією лише особливістю, що гроші в автоматичному режимі видає спеціальний пристрій – банкомат, який і здійснює авторизацію.

Види платіжних карток, основні поняття

ПІН-код – це секретне число, довжина якого становить від 4 до 8 цифр. ПІН генерується і перевіряється спеціальним криптографічним обладнанням. Під час генерації він друкується в закритому конверті, що потім передається власнику карти. *ПІН-конверт* – єдине місце, де цей код перебуває в «чистому» вигляді. У момент генерації випадкового ПІН-коду і друку ПІН-конверта в базу даних емітента криптообладнанням передається перевірочне значення ПІН-коду (*PIN Verification Value*). За допомогою цього значення, а також отриманого в авторизаційному запиті ПІН-блоку (зашифрованого значення ПІН) авторизаційний хост робить запит до криптообладнання, що видає відповідь про правильність уведення цього коду. У такий спосіб відкрите значення ПІН-коду ніде не зберігається і не передається жодними транспортними магістралями. Можливі й інші криптосхеми, що не порушують згаданих принципів безпеки.

На жаль, більша частина криптотехнологій, застосовуваних у роботі з пластиковими картками, є закритою.

Види платіжних карток, основні поняття

При здійсненні розрахунків власник картки обмежений низкою *лімітів*. Характер лімітів і умови їхнього використання можуть бути дуже різноманітними. Однак загалом усе зводиться до двох основних сценаріїв:

– власник дебетової картки повинен заздалегідь внести на свій рахунок у банку-емітенті певну суму. Її розмір і визначає ліміт доступних коштів. При здійсненні розрахунків з використанням картки синхронно зменшується і ліміт. Ліміт контролюється при проведенні авторизації, що у разі використання дебетової картки є обов'язковим завжди. Для поновлення (чи збільшення) ліміту власнику картки необхідно знову внести кошти на свій рахунок;

– для забезпечення платежів власник картки може не вносити попередньо кошти, а одержати в банку-емітенті кредит. Така схема реалізується при оплаті за допомогою кредитної картки. У цьому разі ліміт пов'язаний з розміром наданого кредиту, у рамках якого власник картки може витрачати кошти. Кредит може бути як одноразовим, так і поновлюваним. Поновлення кредиту залежно від договору з власником картки відбувається після погашення або всієї суми заборгованості, або якоїсь її частини.

Види платіжних карток, основні поняття

Як кредитна, так і дебетова картки можуть бути також корпоративними. Корпоративні картки надаються компанією своїм працівникам для оплати витрат у відрядженні або інших службових витрат. Корпоративні картки компанії пов'язані з якимось одним її рахунком. Картки можуть мати розподілений і нерозподілений ліміти. У першому випадку кожному з власників корпоративних карт встановлюється індивідуальний ліміт. Другий варіант більш прийнятний для невеликих компаній і не припускає розмежування ліміту. Корпоративні картки дають змогу компанії детально відслідковувати службові витрати працівників.

Сімейні картки у певному сенсі аналогічні корпоративним – право здійснення платежів у рамках установленого ліміту надається членам родини власника картки. При цьому додатковим користувачам надаються окремі персоналізовані картки.

Платіжна система

Платіжною системою називають сукупність методів і суб'єктів, які її реалізовують, що забезпечують у рамках системи умови для використання банківських пластикових карток обумовленого стандарту як платіжного засобу.

Одне з основних завдань, вирішуваних при створенні платіжної системи, полягає у розробці і дотриманні загальних правил обслуговування карток емітентів, що входять до системи, здійснення взаєморозрахунків і платежів. Ці правила охоплюють як суто технічні аспекти операцій з картками – стандарти даних, процедури авторизації, специфікації на використовуване устаткування тощо, так і фінансові аспекти обслуговування карток – процедури розрахунків з підприємствами торгівлі і сервісу, що входять до складу приймальної мережі, правила взаєморозрахунків між банками, тарифи та ін.

З організаційної точки зору ядром платіжної системи є асоціація банків, що спирається на договірні зобов'язання. До складу платіжної системи також входять підприємства торгівлі і сервісу, що утворюють мережу точок обслуговування. Для успішного функціонування платіжної системи необхідні і спеціалізовані нефінансові організації, що здійснюють технічну підтримку обслуговування карток: процесингові та комунікаційні центри, центри технічного обслуговування тощо.

Платіжна система

Процесинговий центр – спеціалізована сервісна організація, яка забезпечує обробку запитів на авторизацію, що надходять від еквайєрів (чи безпосередньо з точок обслуговування), та/або протоколів транзакцій – зафіксованих даних про виконані за допомогою карток платежі та видачі готівки. Для цього центр веде базу даних, що, зокрема, містить дані про банки – членів платіжної системи і про власників карток.

Центр зберігає інформацію про ліміти власників карток і виконує запити на авторизацію в тому разі, якщо банк-емітент не веде власної бази (offline банк). В іншому разі (online банк) процесинговий центр пересилає отриманий запит до банку-емітента картки, яка авторизується. Очевидно, що центр забезпечує і пересилання відповіді банку-еквайєру. Крім того, на підставі накопичених за день протоколів транзакцій процесинговий центр розраховує і розсилає підсумкові дані для здійснення взаєморозрахунків між банками-учасниками платіжної системи, а також формує і розсилає банкам-еквайєрам стоп-листи.

Процесинговий центр може також забезпечувати потреби банків-емітентів у нових картках, здійснюючи їх замовлення на заводах і подальшу персоналізацію. Розгалужена платіжна система може мати кілька процесингових центрів, роль яких на регіональному рівні можуть виконувати і банки-еквайєри.

Платіжна система

Комунікаційні центри забезпечують суб'єктам платіжної системи доступ до мереж передачі даних. Використання спеціальних високопродуктивних ліній комунікації зумовлено необхідністю передачі великих обсягів даних між географічно розподіленими учасниками платіжної системи при авторизації карток у торговельних терміналах, при обслуговуванні карток у банкоматах, при виконанні взаєморозрахунків між учасниками системи та в інших випадках.

Технічні засоби.
Способи ідентифікації пластикових карток

Пластикова картка являє собою пластину стандартних розмірів (85,6 х 53,9 х 0,76 мм), виготовлену зі спеціальної, стійкої до механічних і термічних впливів, пластмаси. Одна з основних функцій пластикової картки – забезпечення ідентифікації особи, що її використовує, як суб'єкта платіжної системи. Для цього на пластикову картку наносяться логотипи банку-емітента і платіжної системи, що обслуговує картку, ім'я власника картки, номер його рахунка, термін дії картки та ін.

Крім цього, на картці можуть бути фотографія власника та його підпис. Буквено-цифрові дані – ім'я, номер рахунка та інші – можуть бути ембосовані, тобто нанесені рельєфним шрифтом.

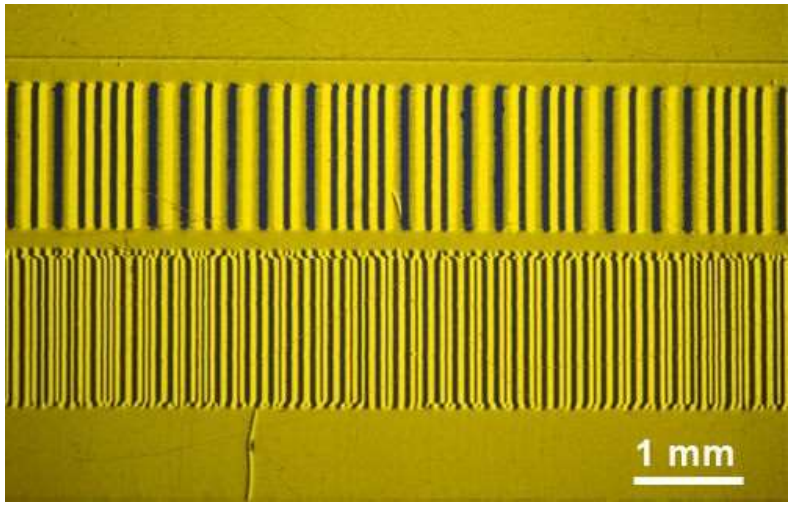
Це дає можливість при ручній обробці прийнятих до оплати карток швидко перенести дані на чек за допомогою спеціального пристрою імпринтера, що прокатує картку (так само, як виходить другий екземпляр при використанні копіювального паперу).

Технічні засоби.
Способи ідентифікації пластикових карток

Графічні дані забезпечують можливість візуальної ідентифікації картки. Картки, обслуговування яких базується на такому принципі, можуть з успіхом використовуватися в малих локальних системах – як клубні, магазинні картки тощо. Однак для використання в банківській платіжній системі візуальної «обробки» виявляється явно недостатньо. Доцільно зберігати дані на картці у вигляді, що забезпечує здійснення процедури автоматичної авторизації. Це завдання може бути вирішене з використанням різних фізичних механізмів. У картках зі штрих-кодом як ідентифікуючий елемент використовується штриховий код, аналогічний коду для маркування товарів. Зазвичай кодова смужка покрита непрозорим складом, і зчитування коду відбувається в інфрачервоних променях. Картки зі штрих-кодом дуже дешеві і порівняно з іншими типами карт відносно прості у виготовленні. Остання особливість зумовлює їхню слабку захищеність від підробки, через що вони малопридатні для використання в платіжних системах.

Технічні засоби.
Способи ідентифікації пластикових карток

Картки з магнітною стрічкою є на сьогодні найпоширенішими – в обігу перебуває понад два мільярди карток цього типу. Магнітна стрічка розташовується на зворотному боці картки і, відповідно до стандарту ISO 7811, складається з трьох доріжок. З них перші дві призначені для зберігання ідентифікаційних даних, а на третю можна записувати інформацію (наприклад, щодо поточного значення ліміту дебетової картки). Однак через невисоку надійність багаторазово повторюваного процесу запису/зчитування запис на магнітну смугу, як правило, не практикується, і такі картки використовуються тільки в режимі зчитування інформації. Захищеність карток із магнітною смугою значно вища порівняно з картками зі штрих-кодом. Однак і такий тип карток відносно вразливий для шахрайства. Проте розвинена інфраструктура існуючих платіжних систем і насамперед світових лідерів «карткового» бізнесу – компаній MasterCard/Europay є причиною інтенсивного використання карток з магнітною смугою і сьогодні.



Технічні засоби.
Способи ідентифікації пластикових карток

Для підвищення захищеності карток системи VISA і MasterCard/Europay використовують додаткові графічні засоби захисту: голограми і нестандартні шрифти для ембосування. На лицьовому боці картки з магнітною смугою, як правило, зазначають:

– логотип банку-емітента;

– логотип платіжної системи;

– номер картки (перші шість цифр – код банку, наступні дев’ять – банківський номер картки, остання з цих цифр – контрольна), в якому останні чотири цифри нанесено на голограму;

– термін дії картки;

– ім’я власника картки.

На зворотному боці картки є таке:

– магнітна смуга;

– місце для підпису.

Технічні засоби.
Способи ідентифікації пластикових карток

Для цього типу карти інформація заноситься на магнітну смугу. Карти з магнітною смугою бувають трьох форматів: ID-1, ID-2, ID-3 (найпоширеніший формат ID-1). Магнітна смуга містить 3 доріжки (найчастіше використовують лише 2), на які в закодованому вигляді записують номер картки, термін її дії, прізвище власника картки тощо. Найбільш повно і точно карти з магнітною смугою описані у стандартах:

- ✓ ISO-7810 «Ідентифікаційні картки – фізичні характеристики»;
- ✓ ISO-7811 «Ідентифікаційні картки – методи запису»;
- ✓ ISO-7812 «Ідентифікаційні картки – система нумерації та процедура реєстрації ідентифікаторів емітентів» (5 частин);
- ✓ ISO-7813 «Ідентифікаційні картки – картки для фінансових транзакцій»;
- ✓ ISO-4909 «Банківські карти – зміст третьої доріжки магнітної смуги»;
- ✓ ISO-7816 «Ідентифікаційні картки – картки з мікросхемою з контактами» (6 частин)

Технічні засоби.
Способи ідентифікації пластикових карток

Гібридна карта з чіпом (смарт-картка). На відміну від карток з магнітною смугою, під час здійснення транзакцій задіюється саме інформація з чіпа. Чіп має великий обсяг пам'яті, і інформація на ньому піддається більш складному типу шифрування. При здійсненні транзакції карткою з магнітною смугою вона завжди має однакові ідентифікуючі карту дані, які передаються в банк. Тому їх можна скопіювати та виготовити підроблену карту.

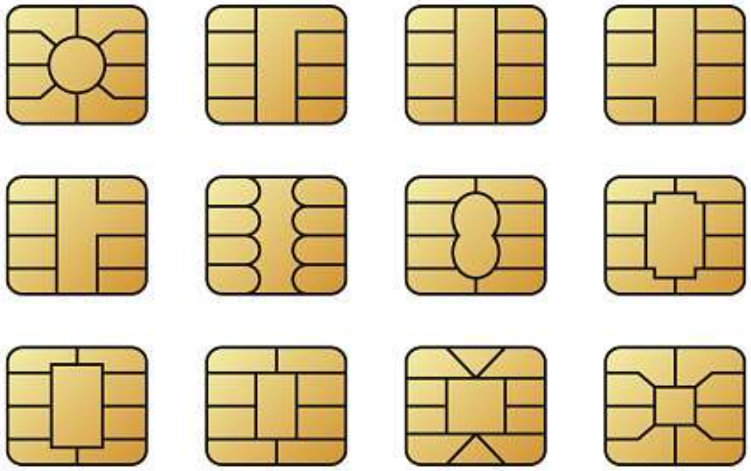
Мікропроцесорна карта працює інакше: кожна транзакція підтверджується спеціально сформованим для неї кодом, і для кожної наступної операції потрібен новий код, зробити дублікат практично неможливо. Гібридний варіант прижився через складний перехід техніки приймаючої карти на новий тип даних. Зараз чіпи вміють читати практично всі пристрої, що приймають пластикові карти.

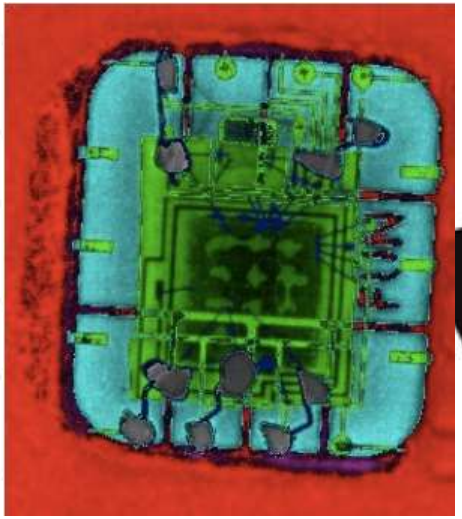
Цікаво: Якщо банкомат провів операцію з використанням лише даних з магнітної смуги, то цю транзакцію можна оскаржити і банк (власник застарілого банкомату) зобов'язаний відшкодувати збитки, завдані власнику картки.

Технічні засоби. Особливості будови смарт-карток

У *смарт-картках* (картках пам'яті) носієм інформації є мікросхема. У найпростіших з існуючих смарт-карток обсяг пам'яті може мати величину від 32 байтів до 16 кілобайтів. Ця пам'ять може бути реалізована або у вигляді НПЗП (EPROM), що допускає одноразовий запис і багаторазове зчитування, або у вигляді ЕННПЗП (EEPROM), що допускає як багаторазове зчитування, так і багаторазовий запис.

Пам'ять смарт-карток буває незахищеною (з повним доступом) або захищеною. У картках першого типу немає жодних обмежень на зчитування і запис даних. Доступність усієї пам'яті робить їх зручними для моделювання довільних структур даних, що є важливим в окремих застосунках. Картки з захищеною пам'яттю мають область ідентифікаційних даних і одну чи кілька прикладних областей.





Технічні засоби. Особливості будови смарт-карток

Ідентифікаційна область карток припускає лише одноразовий запис під час персоналізації і надалі доступна тільки для зчитування. Доступ до прикладних областей регламентується і здійснюється за пред'явленням відповідного ключа. Рівень захисту карток пам'яті вищий, ніж магнітних карток, і вони можуть бути використані в прикладних системах, у яких фінансові ризики, пов'язані з шахрайством, відносно невеликі. Що ж стосується вартості карток пам'яті, то вони дорожчі, ніж магнітні картки. Однак останнім часом ціни на них значно знизилися в зв'язку з удосконаленням технології і зростанням обсягів виробництва. Вартість картки пам'яті безпосередньо залежить від вартості мікросхеми, зумовленої, у свою чергу, місткістю пам'яті.

Окремим зразком карток пам'яті є карти-лічильники, в яких значення, збережене в пам'яті, може змінюватися лише на фіксовану величину. Такі картки використовуються в спеціалізованих застосунках з передоплатою (плата за використання телефону-автомата, оплата автостоянки тощо).

Технічні засоби. Особливості будови смарт-карток

Картки з мікропроцесором являють собою по суті мікрокомп'ютери і містять усі відповідні основні апаратні компоненти: центральний процесор, ОЗП, ПЗП, НПЗП, ЕННПЗП. Параметри найпотужніших сучасних мікропроцесорних карток порівнянні з характеристиками персональних комп'ютерів початку 80-х років XX ст.

Операційна система, що зберігається в ПЗП мікропроцесорної картки, принципово нічим не відрізняється від операційної системи ПК і надає великий набір сервісних операцій і засобів безпеки. Операційна система підтримує файлову систему, що базується в ЕЗНПЗП (місткість якої, як правило, перебуває в діапазоні 1–8 кБт, але може досягати і 128 кБт), і забезпечує регламентацію доступу до даних. При цьому частина даних може бути доступна тільки внутрішнім програмам картки. Це разом із вбудованими криптографічними засобами робить мікропроцесорну картку високозахищеним інструментом, що може бути використаний у фінансових застосунках, які висувають підвищені вимоги до захисту інформації. Саме тому мікропроцесорні картки (і смарт-картки взагалі) розглядають нині як найперспективніший вид пластикових карток.

Крім того, смарт-картки є найперспективнішим типом пластикових карток також і з точки зору функціональних можливостей. Обчислювальні можливості смарт-карток дають змогу використовувати, наприклад, ту саму картку і в операціях з online авторизацією, і як багатовалютний електронний гаманець. Їх широке використання в системах VISA і Europay/MasterCard вже почалося, а протягом десятиріччя смарт-картки повинні цілком витіснити картки з магнітною смугою.

Використання POS-терміналів

POS-термінали, або торгові термінали, призначені для обробки трансакцій при фінансових розрахунках з використанням пластикових карток з магнітною смугою і смарт-карток. Використання POS-терміналів дає можливість автоматизувати операції з обслуговування картки та істотно зменшити час обслуговування.

Можливості і комплектація POS-терміналів варіюються в широких межах, однак типовий сучасний термінал укомплектовано пристроями читання як смарт-карток, так і карток із магнітною смугою, а також енергонезалежною пам'яттю, портами для підключення ПІН-клавіатури (клавіатури для набору ПІН-коду), принтера, з'єднання з ПК чи електронним касовим апаратом. Крім того, зазвичай POS-термінал буває оснащений модемом з можливістю автододзвону.

Використання POS-терміналів

POS-термінал має «інтелектуальні» можливості – його можна програмувати. Як мови програмування використовуються асемблер, а також діалекти C і Basic. Усе це дає змогу не тільки здійснювати online-авторизацію карток із магнітною смугою і смарт-карток, а й використовувати при роботі зі смарт-картами режим offline з накопиченням протоколів транзакцій. Останні під час сеансів зв'язку передаються у процесинговий центр.

Під час сеансу зв'язку POS-термінал може також приймати і запам'ятовувати інформацію, передану ЕОМ процесингового центру. Найчастіше це бувають стоп-листи, але у такий спосіб можна і перепрограмувати POS-термінали. Вартість POS-терміналів залежно від комплектації, можливостей, фірми-виробника може коливатися від кількох десятків до кількох тисяч доларів. Розміри і вага POS-термінала порівнянні з аналогічними параметрами телефонного апарата, а найчастіше бувають меншими.

Атаки на смарт-картки

Перед розробниками було поставлено завдання створення пристрою для роботи з конфіденційною інформацією за умов ворожого середовища. Результатом їхньої роботи є смарт-картки – високоінтегровані захищені пристрої. Безпека даних та програм застосунків забезпечується за рахунок контролю доступу до інформації в пам'яті смарт-карт. Принципи проектування, безпека застосунків, апаратне забезпечення мікроконтролера, алгоритми програмного забезпечення операційної системи все це тією чи іншою мірою впливає на безпеку смарт-карток.

Смарт-карта є безпечною при коректній спільній роботі захисних механізмів корпусу карти, чіпа (апаратного забезпечення), операційної системи, застосунка. У разі виходу з ладу хоча б одного з цих компонентів або незадоволення вимог до певного компонента гарантувати безпеку смарт-карти вже неможливо.

Атаки на смарт-картки. Види атак

З метою класифікації атак щодо часу їхнього проведення можуть використовуватися фази життєвого циклу смарт-картки. У цьому випадку класифікація таких атак матиме такий вигляд:

- Атаки на етапі розробки смарт-карт;
- Атаки на етапі виробництва смарт-карт;
- Атаки на етапі застосування смарт-карт.

Розглянемо наступну класифікацію атак більш детально:

- ✓ Атаки на соціальному рівні;
- ✓ Атаки на фізичному рівні;
- ✓ Атаки на логічному рівні.

Атаки на смарт-картки. Види атак

Атаки на соціальному рівні мають на увазі під собою атаки на людей, які працюють зі смарт-картками незалежно від фази життєвого циклу смарт-картки. Головну роль у процесі відбиття та запобігання атакам даного типу є організаційні заходи безпеки, технічні заходи відіграють тут другорядну роль. Організаційні заходи безпеки можуть полягати в установці непрозорих екранів по обидва боки клавіатури, тим самим унеможливлюється підглядання pin-коду. Одним із організаційних заходів з метою запобігання атакі даного типу на програмістів є регламентація у відповідних документах розробки та використання відкритих процедур програмістами смарт-карток. Ступінь безпеки в даному варіанті визначатиметься секретними ключами.

Атаки на смарт-картки. Види атак

Щодо **фізичних атак** необхідно чітко усвідомити, що у зв'язку з необхідністю у фізичному доступі до апаратних засобів мікроконтролера смарт-карти, зловмиснику знадобиться складне технічне обладнання. Дані атаки можуть бути статичними, або динамічними. Згадані підвиди атак фізично мають дві важливі різницю між собою. Здійснення статичних атак зловмисником не вимагає наявність працюючого мікроконтролера і не накладає часових обмежень на зловмисника. Динамічні атаки диктують зловмиснику чіткі умови: працюючий мікроконтролер, певне вимірювальне обладнання та високу швидкість обробки даних.

Атаки на смарт-картки. Види атак

Існує три основні види фізичних атак:

1. **Пасивні атаки** (passive attacks). До них відносяться атаки, що базуються на спостереженні за будь-яким фізичним параметром реалізації, промодульованим ключовою інформацією. Прикладами пасивних атак є атаки за енергоспоживанням (SPA і DPA – differential power analysis і simple power analysis), атаки за часом (timing attacks) та атаки з електромагнітного випромінювання. Пасивні атаки відносно добре вивчені та докладно висвітлені у відкритій літературі. Однак існує й збалансована система заходів протидії цим атакам.

2. **Активні атаки без проникнення** (active non-invasive attacks). До цього класу відносяться атаки, засновані на генерації випадкових апаратних помилок під час виконання криптоалгоритму та подальшого їх аналізу. Класичним прикладом таких атак є диференціальні атаки на основі наведення апаратних помилок (DFA – differential fault analysis) та енергетичні атаки (energy attacks), що включають маніпуляцію тактовими сигналами і постачання мікросхеми енергією (glitching), вплив лазером або пучком, інші методи. Проте, на відміну від пасивних атак, для DFA, наприклад, відсутня відпрацьована практична модель захисту. На даний момент фірми-виробники смарт-карт ведуть інтенсивну розробку таких моделей та конкретних механізмів.

3. **Активні атаки з проникненням** (active invasive attacks). Тут йдеться про атаки на мікросхеми із проникненням у саму мікросхему. Прикладами таких атак є атаки на основі проб (probe attacks), часто комбіновані з різними методами зняття корпусу мікросхеми та пошарового доступу до топології кристала (machining methods) та інші атаки. Активні атаки з проникненням традиційно є ноу-хау лише невеликої кількості комерційних та урядових організацій. Лише мала частка цієї інформації публікується.

Атаки на смарт-картки. Види атак

Атаки на логічному рівні здійснюються за рахунок класичного криптоаналізу, відомих несправностей операційної системи смарт-карти, «троянських коней» у коді застосунків смарт-карти, що виконується. За статистикою, дані атаки є найбільш успішними.

Насправді ж іноді здійснюються і атаки змішаного типу.

Атаки на смарт-картки. Деякі способи протидії

Основна відмінність контактних та безконтактних смарт-карток з точки зору безпеки – це наявність у безконтактних смарт-карток радіочастотного каналу зв'язку картки та зчитувача, наслідком появи якого є можливість здійснення нових атак. Наприклад, підслуховування, результатом якого може стати створення абсолютної копії повноцінної картки. Запобігання прослуховування полягає в аутентифікації та шифруванні даного каналу зв'язку, перериванні роботи, уникнути якого можна використанням механізмів доведення транзакції до логічного кінця; відмови в обслуговуванні, захистом якого може бути наявність у застосунків сертифікатів терміналів, руйнування карти на відстані за допомогою руйнівного електромагнітного поля.

Мікропроцесорний чіп сучасного виробництва має програмний, апаратний, технологічний рівні захисту від несанкціонованого доступу щодо інформації, що міститься в ньому.

Програмний рівень захисту містить у собі такі методи та засоби захисту операційної системи:

- ✓ контроль доступу шляхом завдання відповідних правил, призначення атрибутів файлів, блокування файлів, каталогів, карти;
- ✓ захист pin-кодом;
- ✓ взаємна автентифікація картки та терміналу;
- ✓ шифрування команд, даних, каналу обміну.

Атаки на смарт-картки. Деякі способи протидії

При створенні прикладних інформаційних систем зі смарт-картами повинні враховуватися рекомендації, наведені у специфікації PC/SC щодо безпеки взаємодії смарт-карток та персональних комп'ютерів. Стандарт ISO 7816 для смарт-карток – основа інтегрованої технології PC/SC. Один із розділів даної специфікації регламентує наявність у смарт-карток криптографічних сервісів з метою убезпечити взаємодію смарт-карток з персональними комп'ютерами. Передбачені такі криптографічні послуги:

- ✓ алгоритми симетричного шифрування;
- ✓ алгоритми хешування;
- ✓ алгоритми цифрового підпису;
- ✓ алгоритми розподілу криптографічних ключів;
- ✓ засоби генерації випадкових чисел;
- ✓ засоби генерації карткою ключів для алгоритмів симетричного шифрування та цифрового підпису;
- ✓ сервіси аутентифікації.

Також у специфікації PC/SC чітко передбачено створення сервісів зберігання даних відповідно до стандарту ISO/IEC 7816–4 та створення окремих файлів для зберігання ключів, секретів, констант, даних аутентифікації.

Атаки на смарт-картки. Деякі способи протидії

Основою забезпечення безпеки програм смарт-карт є захисні механізми операційної системи та апаратного забезпечення. Процедури автентифікації значно підвищують безпеку програм смарт-карт.

Pin-код – це не лише найпоширеніший метод ідентифікації користувача смарт-картки, але й єдиний спосіб захисту від несанкціонованого доступу у разі втрати, крадіжки чи підробки смарт-картки.

Практично, на pin-код зловмисник може здійснити дві атаки: підглядання та вгадування. Імовірність вгадування залежить від таких параметрів pin-коду:

- ✓ Довжина
- ✓ Символи, що входять до нього;
- ✓ Кількість дозволених неправильних спроб введення, після якого введення блокується.

Однак розблокування процесу введення PIN-коду має бути забезпечене незалежним засобом автентифікації.

Якщо у авторизованого користувача виникне бажання перевірити справжність терміналу перед введенням свого PIN-коду, то процедура автентифікації терміналу здійснюється наступним чином: як тільки смарт-карта вставлена в термінал, відбувається процес їх взаємної аутентифікації. Якщо взаємна автентифікація пройшла успішно, смарт-карта дозволяє терміналу доступ до файлу із секретним паролем користувача для подальшого виведення його на екран терміналу. Побачивши свій секретний пароль, користувач може бути впевненим у справжності терміналу.

Атаки на смарт-картки. Деякі способи протидії

Біометричні методи ідентифікації є безпечнішими та зручнішими для користувача в порівнянні з pin-кодами. Також слід звернути увагу на неможливість передачі біометричних ознак іншій людині.

З урахуванням істотного зниження швидкості передачі при реалізації шифрування, рентабельно було б провести чітку градацію між даними, що підлягають і не підлягають шифруванню.

Не варто забувати, що є можливість здійснення атаки безпосередньо на криптографічну систему, а саме, зловмисник спробує обчислити значення секретного ключа. Найбільш простим заходом безпеки від цієї атаки є великий простір ключів криптографічного алгоритму.

З метою захисту від атак із застосуванням диференціального аналізу DFA (differential fault analysis) або потужного аналізу PA (power analysis) до даних додається префікс як випадкове число з подальшим їх шифруванням.

Більшість застосунків застосовують до даних не шифрування, а код аутентифікації повідомлення MAC (Message Authentication Code), атака на який «грубою силою» набагато складніша, ніж на пару «відкритий текст – шифрований текст».

Застосування динамічних ключів, які змінюються кожної операції шифрування, ще більше ускладнить завдання зловмиснику.

Атаки на смарт-картки. Деякі способи протидії

Рекомендації специфікації взаємодії смарт-карт та персональних комп'ютерів PC/SC регламентують реалізацію смарт-картами алгоритмів та можливостей, що підтримують:

- ✓ автентифікацію користувача смарт-карткою;
- ✓ автентифікацію користувача віддаленим об'єктом, практично завжди сервером;
- ✓ автентифікацію програми ПК смарт-картою;
- ✓ аутентифікацію смарт-карти застосунком.

Атаки на смарт-картки. Деякі способи протидії

Аутентифікація користувача смарт-картою, в основному, здійснюється за допомогою PIN-коду.

Аутентифікація користувача віддаленим об'єктом може здійснюватися одним із нижчезазначених протоколів.

Перший протокол – це протокол односторонньої аутентифікації з секретом, який зловмисник може обійти, встановивши контроль над каналом після виконання процедури аутентифікації. Однак якщо привласнити кожному повідомленню код автентифікації MAC, то загрозу буде анульовано.

Другий протокол – це протокол двосторонньої автентифікації з секретом, що розділяється, що забезпечує захищений канал.

Третій протокол – це протокол аутентифікації з використанням цифрового підпису та цифрового сертифіката, що забезпечує аутентифікацію між клієнтом та сервером у відкритих мережах.

Аутентифікація програми ПК смарт-картою здійснюється вище згаданим протоколом аутентифікації з секретом, що розділяється. Цей протокол дає можливість застосунку ПК здійснювати контроль доступу до конфіденційної інформації конкретних користувачів під час її зберігання на смарт-картці.

Аутентифікація смарт-картки застосунком дозволяє провести перевірку достовірності типу та виробника смарт-картки, що, у свою чергу, дозволяє отримати інформацію щодо криптографічної підтримки, загальної захищеності смарт-картки. З цією метою на етапі виробництва в смарт-карту закладаються секретний ключ її виробника, який має бути невилученим, та сертифікат відкритого ключа із закодованим у ньому відкритим ключем виробника.


Дякую за увагу
Лекцію закінчено