УДК 004.087.5

АНАЛІЗ ТЕХНОЛОГІЙ СМАРТ-КАРТ

М.Ф. БОНДАРЕНКО , М.Г. ЗАРОСИЛОВА

На сьогоднішній день смарт-карти грають велику роль в якості “активних” пристроїв безпеки. Завдяки її програмуючої пам’яті та мікрокомп’ютеру, смарт-карти можуть задовольнити специфічні потреби в середовищі, в якій вона буде використовуватись. Смарт-карти дозволяють безпечну обробку і зберігання конфіденційних даних, таких як права користувачів і криптографічні ключі, а також виконання криптографічних алгоритмів. Вони є безпечними маркерами, за допомогою яких користувач може бути ідентифікований та автентифікован комп’ютерною системою або мережею зв’язку і навпаки. Ця стаття знайомить з особливостями чіп-карт, їх життєвим циклом і стандартами, що регулюють їх, моделлю довіри та загроз.

Ключові слова: смарт-карта, мікросхема, модель загроз, модель довіри, життєвий цикл.

ВСТУП

На даному етапі Україна активно впроваджує проект «Соціальна карта» – це впровадження автоматизованих обліково-платіжних систем на основі персоніфікованих електронних пластикових карт, так званих «соціальних карт», в містах України. Така електронна картка зможе виконувати різні функції, зокрема облікову, інформаційну, платіжну та ін. Для забезпечення цих функцій, у якості електронного засобу, була вибрана технологія чіпових карт (смарт-карт).

Отже, основна відповідальність за виконання таких функцій, як цілісність, доступність, конфіденційність, захист від несанкціонованого доступу лягає на смарт-карту.

Таким чином, виникає питання о захищеності таких карток, чи зможуть вони, насправді, забезпечити гідний рівень захисту даних та безпечне виконання різних операцій.

У цій статті ми спробуємо відповісти на це питання за допомогою аналізу технології смарт-карт.

1. ОПИС ТЕХНОЛОГІЇ СМАРТ-КАРТ

Впровадження смарт-карт в інформаційні технології, мабуть, сама захоплююча зміна в цифровій історії. Смарт-карти прийшли на зміну магнітним картам, які вже не можуть забезпечити достатнього рівня безпеки та переживають свій захід.

Термін «смарт-карта» двозначний і використовується багатьма різними способами, однак ISO використовує термін, Integrated Circuit Card (ICC) – картка з інтегрованою схемою , щоб охопити всі ці пристрої, де міститься інтегральна схема.

Карта має розміри 85.6мм х 53.98мм х 0,76 мм такі як і банківські карти з магнітною смугою, що використовується в якості платіжного (рис. 1) [2].

Мікросхема смарт-карти містить “логіку”, що і робить ці картки інтелектуальними, по-англійськи – “smart”. Мікросхеми смарт – картки являють собою повні мікроконтролери (мікрокомп’ютери) і містять такі компоненти:

CPU (центральний процесор) – пристрій для обробки інструкцій картки;

RAM (ОЗУ) – пам’ять для тимчасового зберігання даних, наприклад, результатів обчислень, зроблених процессором;

ROM (ПЗУ) – пам’ять для постійного зберігання інструкцій картки, що виконуються процесором, а також інших даних, які не змінюються. Інформація в ПЗП записується в процесі виробництва карти;

EPROM (ППЗУ) – пам’ять, яка може бути прочитана багато разів, але записана тільки однократно. У ППЗУ організація, що випускає картку в обіг, записує дані про її власника;

EEPROM (ЕСППЗУ) – пам’ять, яка може бути переписана і зчитана багато разів. У цій пам’яті зберігаються змінювані дані власника карти. ППЗУ і ЕСППЗУ не втрачають дані при відключенні живлення;

I/O (Введення/виведення) – система для обміну даними із зовнішнім світом;

Operating system (операційна система або програмне забезпечення картки) – Інструкції для процесора, що зберігаються на карті;

Security features (система безпеки) – вбудована система безпеки для захисту даних з можливістю їх шифрування.

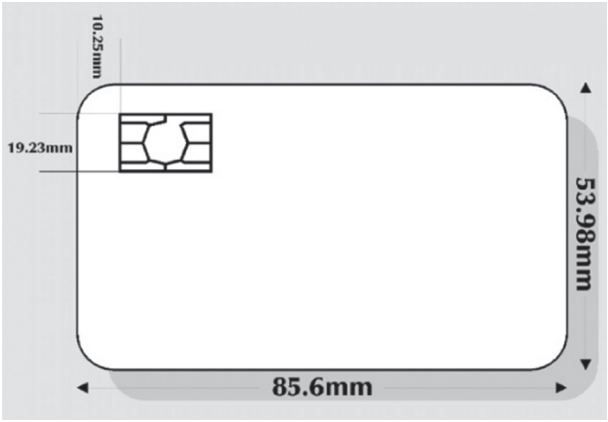

Рис. 1. Вигляд картки, розміри якої визначені стандартом 7816-1

У стандарті ISO 7816 (частини 1-7), затвердженому Міжнародною організацією зі стандартизації (International Standard Organization, ISO), визнача-

ються правила, що регулюють найрізноманітніші аспекти, пов'язані зі смарт-картами. Стандарт ISO 7816 складається з наступних розділів:

1) ISO / IEC 7816-1 Фізичні характеристики (розміри);

2) ISO / IEC 7816-2 Контактні карти – розміщення чіпа і розміри;

3) ISO / IEC 7816-3 Електронні характеристики для контактних карт;

4) ISO / IEC 7816-4 Формат команд і безпека;

5) ISO / IEC 7816-5 Реєстрація виготовлювачів додатків і ідентифікатори додатків;

6) ISO / IEC 7816-6 Міжгалузеві елементи;

7) ISO / IEC 7816-7 Міжгалузеві команди SCQL (Structured Card Query Language) ;

8) ISO / IEC 7816-8 Команди для безпечної передачі даних і різних операцій;

9) ISO / IEC 7816-9 Команди для управління картою;

10) ISO / IEC 7816-10 Електричні сигнали і ATR (Answer To Reset) для синхронних карт;

11) ISO / IEC 7816-11 Верифікація персоналу за допомогою біометричних методів;

12) ISO / IEC 7816-12 Різні характеристики смарт-карт з USB інтерфейсом (USB-ICC) ;

13) ISO / IEC 7816-13 Команди для управління додатками і взаємодією додатків на карті;

14) ISO / IEC 7816-15 Застосування криптометодів.

2. КЛАСИФІКАЦІЯ СМАРТ-КАРТ

Існує декілька видів класифікації смарт-карт (наприклад, за типом мікросхеми, що в ній вбудована і за функціями, які виконує смарт-карта). Найпростіші типи карт містять тільки пам'ять, більш складні є мікро-ЕОМ, яка забезпечує великий набір сервісних функцій. Розглянемо деякі з них [3].

Залежно від типу мікросхеми, вбудованої в карту, розрізняють такі типи смарт-карт:

Картки із програмованим постійним пристроєм для запам'ятовування (EPROM) є найпростішим типом карт. Основна їх застосування – розрахунки за телефонні переговори;

Картки з енергозалежною перепрограмованою пам'яттю (EEPROM) дозволяють перезаписувати інформацію, що зберігається в них. Основна мета їх застосування – зберігання індивідуальних даних;

Картки з захищеною перепрограмованою пам'яттю, які забезпечують доступ для читання/запису тільки після введення спеціального коду. Основна їх застосування – розрахункові карти або зберігання захищених індивідуальних даних.

Багатофункціональні карти містять великий обсяг енергозалежної перепрограмуючої пам'яті, а також спеціальний мікропроцесор і вбудовану операційну систему, що забезпечує набір сервісних функцій. Ці карти можуть застосовуватися для будь-яких додатків, включаючи розрахунки користувача.

За призначенням можна виділити:

Карти-лічильники – застосовуються для такого типу розрахунків, коли потрібно відніманння фіксованої суми за кожну платіжну операцію. Такі картки ще називають передплаченими картками. **Карти пам'яті** – використовуються для зберігання інформації. Сама їхня назва говорить про те, що мікросхема картки містить тільки запам'ятовуючий пристрій. Є два типи таких карток: з захищеної та незахищеної пам'яттю:

– у картах з *незахищеною пам'яттю* немає обмежень по читанню або запису даних. Використовувати такі карти як платіжних карт дуже небезпечно. Досить легально придбати таку картку, скопіювати її пам'ять на диск, а далі після кожної покупки відновлювати її пам'ять копіюванням початкового стану даних з диска. Зрозуміло, що таку операцію може виконати лише кваліфікований програміст, але практика показує, що людей, здатних на це, достатньо;

– у картках із *захищеною пам'яттю* використовується спеціальний механізм для дозволу читання / запису або видалення інформації. Щоб провести ці операції, необхідно ввести спеціальний секретний код (а іноді і не один). Як правило, карти із захищеною пам'яттю містять область, куди записуються ідентифікаційні дані. Ці дані не можуть бути змінені, що дуже важливо для забезпечення неможливості фальсифікації картки. Картки з захищеною пам'яттю можна використовувати, як платіжний засіб, а також для зберігання конфіденційних даних.

Мікропроцесорні карти схожі на карти пам'яті, але мікросхема містить мікропроцесор (чіп-модуль), що робить ці картки дійсно інтелектуальними.

Мікропроцесор – це мікросхема (інтегральна схема, чіп), яка здатна зберігати великий обсяг інформації і виконувати арифметичні та логічні операції. Мікропроцесорні карти, практично є мікрокомп'ютерами з своїм процесором, оперативною і постійною пам'яттю і навіть операційною системою. Як правило, в такі картки вбудовані криптографічні засоби, що забезпечують шифрування інформації.

Мікропроцесори, встановлені на смарт-картах, мають такі основні характеристики:

– тактова частота до 5 МГц;

– обсяг оперативної пам'яті (ОЗП) до 256 байт (для виконання команд);

– обсяг постійної пам'яті (ПЗУ) до 10 Кбайт (для зберігання операційної системи);

– ємність перезаписувати енергозалежну пам'яті до 8 Кбайт.

У картку вбудовується спеціалізована операційна система, що забезпечує великий набір сервісних операцій і засобів безпеки.

Операційна система карти підтримує файлову систему, що передбачає розмежування доступу до інформації. Для інформації, що зберігається в будь-якому записі (файл, група файлів, каталог), можуть встановлюватися такі режими доступу:

– завжди доступна для читання/запису. Цей режим дозволяє читання/запис інформації без знання спеціальних секретних кодів;

– доступна для читання, але вимагає спеціальних повноважень для запису. Цей режим дозволяє вільне читання інформації, але дозволяє запис тільки після введення спеціального секретного коду;

– спеціальні повноваження для читання запису – цей режим дозволяє доступ для читання або запису після пред'явлення спеціального секретного коду, причому коди для читання і запису можуть бути різними;

– недоступна – цей режим не дозволяє читати або записувати інформацію. Інформація доступна тільки внутрішнім програмам картки. Зазвичай цей режим встановлюється для записів, що містять криптографічні ключі.

Карти забезпечують різний спектр сервісних команд. Для банківської діяльності це засоби ведення електронних платежів. До спеціальних засобів належать можливість блокування роботи з картою. Розрізняють два види блокування при пред'явленні неправильного транспортного коду і при несанкціонованому доступі.

Суть транспортного блокування полягає в тому, що доступ до картки неможливий без пред'явлення спеціального транспортного коду. Цей механізм необхідний для захисту від нелегального використання карток при розкраданні під час пересилання карти від виробника до споживача. Картка може бути активізована тільки при пред'явленні правильного транспортного коду.

Суть блокування при несанкціонованому доступі полягає в тому, що якщо при доступі до інформації кілька разів неправильно був пред'явлений код доступу, то картка взагалі перестає бути працездатною. При цьому, залежно від встановленого режиму, картка може бути згодом або активізована при пред'явленні спеціального коду, або ні. В останньому випадку картка стає непридатною для подальшого використання.

Карти оптичної пам'яті були винайдені в 1981 р. Вони мають велику ємність, чим карти пам'яті, але дані на них можуть записуватися тільки один раз. У таких картках використовується WORM-технологія (одноразова запис – багаторазове читання). Запис і читання інформації з такої картки проводиться спеціальною апаратурою з використанням лазера (звідки інша назва – **лазерна карта).** Технологія, використана в картках, подібна до тієї, яка використовується в лазерних дисках.

Основна перевага таких карток – можливість зберігання великих обсягів інформації.

Прикладом **Суперсмарт-карти** може служити багатоцільова картка фірми Toshiba, використовувана в системі VISA. Крім всіх можливостей звичайної смарт-карти, ця карта має невеликий дисплей і допоміжну клавіатуру для введення даних. Ця карта поєднує в собі кредитну, дебетову карти, а також виконує функції годинника, календаря, калькулятора, здійснює конвертацію валюти, може служити записником і т.д. Через високу вартість суперсмарт-карти не отримали сьогодні широкого поширення, але їх використання буде рости, оскільки вони дуже перспективні.

За доступом розрізняють контактні і безконтактні смарт-карти:

Найбільше поширення сьогодні отримали **контактні карти.** При установці карти в рідер, металеві контакти, розташовані на поверхні картки, стикаються (механічний контакт) з контактами рідера, після чого між ними може здійснюватися обмін інформацією. Вимоги до таких карток встановлює серія стандартів ISO/IEC 7816.

Безконтактні картки – різновид смарт-карт із вбудованою антеною і безконтактним інтерфейсом, що забезпечує взаємодію карти і рідера на невеликій відстані при харчуванні чіпа картки за допомогою електромагнітного поля. Набули широкого поширення в системах контролю фізичного доступу і на транспорті, а також в якості соціальних карт.

Безконтактні пластикові картки є одним з основних елементів систем радіочастотної ідентифікації об'єктів (RFID – систем), які працюють на відстані від рідера (разом з чіпом у пластиковій картці розміщується антена, за допомогою якої проводиться приймання і випромінювання радіохвиль).

Основними перевагами безконтактних пластикових карт є:

– висока надійність і необмежений ресурс карти (забезпечується відсутністю необхідності механічного контакту між картою і рідером);

– велика швидкість обміну інформацією між картою і рідером (мсек);

– можливість багаторазового використання (читання – необмежена кількість разів, перезапис – до 100 000 разів);

– висока надійність зберігання інформації (інформація на карті не схильна до впливу зовнішніх полів і може зберігатися до 10 років);

– високий ступінь захисту від підробок (картку практично неможливо підробити);

– можливість багатофункціональності безконтактних пластикових карток (картки можуть нести великий обсяг перезаписувати інформації і використовуватися одночасно для цілого ряду додатків).

Зазначені вище переваги безконтактних пластикових карт визначають сферу їх застосування. Типові з них:

– електронний контроль доступу та облік часу робітника, персоналу підприємств та організацій;

– системи платного доступу на різні об'єкти (атракціони, тренажерні зали, підйомники і т.д.);

– системи електронних платежів за користування різними видами громадського транспорту;

– системи електронних платежів за послуги для власників транспортних засобів (розрахунки на АЗС, автостоянках, платних дорогах і т.д.);

- системи захисту та сигналізації на транспортних засобах;

- системи лояльності покупців;

- платежі за послуги і товари (електронний гаманець).

Крім цього, існують **комбіновані смарт-карти** і смарт-карти з дуальним інтерфейсом. Комбіновану смарт-картка – просте фізичне об'єднання на одній карті двох чіпів – одного з контактним та іншого – з безконтактним інтерфейсом. Один з одним ці чіпи ніяк не пов'язані. Смарт-карти з дуальним інтерфейсом мають один чіп, доступ до його пам'яті можливий як через контактну площадку, так і "через повітря" – безконтактним шляхом.

Основним документом для безконтактних карт служить серія стандартів для безконтактних карт ISO/IEC 14443:

1) ISO/IEC 14443-1 Фізичні характеристики

2) ISO/IEC 14443-2 Електромагнітні хвилі, сигнали і інтерфейси

3) ISO/IEC 14443-3 Ініціалізація (при наближенні карти до зчитуючого пристрою) і антиколізія (робота з декількома безконтактним картами на одному зчитуючому пристрої)

4) ISO / IEC 14443-4 Протоколи передачі даних.

3. МОДЕЛЬ ДОВІРИ

Розглянемо сторони,які потенційно беруть участь у будь-якій системі, заснованій на смарт-картах. Як правило, їх п'ять чи шість, включаючи: власника карти, термінал, власника даних, виробника карт і виробника ПО [1].

Виділяють наступні сторони:

• Власник картки – це сторона, яка володіє смарт-картою. У випадку, коли смарт-карта використовується як електронний гаманець, він є особою, якій був виданий гаманець. Він може контролювати дані на карті, в залежності від системи, але дуже малоймовірно, що він має контроль над протоколами, ПЗ або робити вибір у створенні апаратного засоби у створенні карткової системи.

• Власник даних – це сторона, яка здійснює контроль даних в карті. У таких випадках як використання карти в якості механізму для проведення цифрового підпису, власник карти так само є власником даних. Однак, якщо картка – електронно-грошова, емітентом грошових коштів є власник даних, і це відкриває можливість атаки.

• Термінал – це пристрій, який пропонує смарт-картці взаємодіяти зі світом. Термінал контролює всі пристрої вводу\виводу в і з смарт-карти: клавіатуру, з допомогою якої дані вводяться на смарт-карту, екран, за допомогою якого будь-які дані з смарт-карти відображаються. Якщо смарт-карта використовується як телефонна, то в ролі терміналу виступає власник телефонного автомата. Якщо картка використовується як АТМ ідентифікаційна карта, то в ролі терміналу виступає АТМ постачальник послуг. Якщо картка використовується як платна карта TV членства, то в ролі терміналу виступає – термінал телеприставки.

• Емітент картки – сторона, яка видає смарт-карти. Ця сторона контролює операційну систему працює на карті, і будь-які дані, які спочатку зберігаються на смарт-картці. Якщо це карта телефонної оплати, то емітент – телефонна компанія. Якщо це ідентифікаційна карта співробітника, то емітент – роботодавець. Іноді емітент лише видає картку і потім зникає з системи; в іншому випадку – він пов'язаний з системою всюди. У деяких багатофункціональних картах, емітент картки може не мати нічого спільного з додатками працюють на карті, і може керувати тільки ОС. У іншим багатофункціональних картах, один і той же емітент може контролювати всі додатки на карті.

З точки зору аналізу безпеки, частіше розглядають емітента карт, виробника і розробників програмного забезпечення як один бік; втім, якими і вони рідко є. Отже:

• Виробник карти – це сторона, яка виготовляє смарт-карти. Відзначимо, що це спрощення; виробник може мати і не мати виробництва з виготовлення чіпів; вони можуть мати договір із субпідрядником на розробку функцій, і можуть використовувати сторонні інструменти в їх роботі, такі як VHDL компілятори. Тим не менш, ми моделюємо це все як виробництво карток. Можливості підірвати виробництво карт відбувається з безлічі місць, для широкого кола осіб.

• Виробник ПЗ – сторона, яка випускає ПЗ для смарт-карт.

4. ЖИТТЄВИЙ ЦИКЛ

Багато хто вважає, що «життя» карти починається з моменту отримання її власником, але насправді це не так, воно починається задовго до цього, а саме з її виробництва

Розглянемо життєвий цикл виробництва карти (рис. 2).

Етапи на рис. 2. можна описати як:

• Розробка вбудованого ПЗ

Усе ПЗ на смарт-картці може розглядатися як вбудоване. Однак, воно може бути розділене на "спеціалізоване ПЗ", яке здійснюється в рамках ІС (наприклад, само-тестування ПЗ), ПЗ операційної системи та прикладного ПЗ. Спеціалізоване, як правило, виробляється заводом-виробником ІС, і зберігається в ПЗУ.

ПЗ для ОС інтегральної схеми може бути написане виробником або третьою стороною, і зберігається в основному в ROM. Деякі оновлення для ОС або спеціальних даних (наприклад, ключів) можуть бути проведені в EEPROM (або іншій енергонезалежній пам'яті), замість в ROM.

Прикладне ПЗ, може зберігатися в ROM, якщо воно є досить загальним, і якщо воно доступне на момент виробництва ІС, таким чином зберігання прикладного ПЗ в ПЗУ часто використ-

товується для того, щоб залишити більше енергонезалежній пам'яті (для встановлення додаткових додатків та/або додаткових даних).

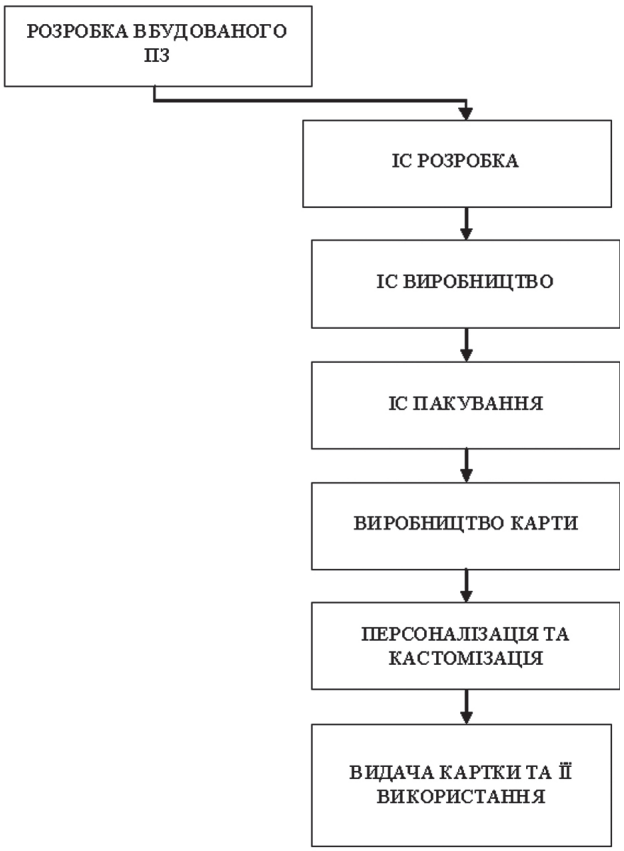

Рис. 2. Життєвий цикл виробництва смарт-карти

• ІС розробка

На цій стадії виробляється апаратний засіб для смарт-карт. У більшості випадків ця конструкція не є якоюсь специфічною для системи на смарт-картах, вона для загального призначення, але потім на неї буде встановлено ОС та різне додаткове ПЗ, яке буде визначати її призначення.

• ІС виробництво

На стадії виробництва відбувається ІС розробка та ПЗ, яке буде зберігатися в ПЗУ (поєднання спеціального ПЗ, операційної системи і, можливо, прикладного ПЗ). Потім ІС виготовляється у формі пластини та випробовується.

Також ця стадія може включати введення даних в EEPROM. Ці дані можуть включати: ідентифікаційні дані для конкретних ІС – ключі та інші дані, пов'язані з схемою та/або системою. Ці дані можуть бути критично важливі для безпеки, і система може мати чітко визначені процедури для безпечного формування, доставки, зберігання і використання даних.

• ІС пакування

Пластини розрізають на окремі мікросхеми та пакують в відсік для вставки в карту. Це включає в себе з'єднання колодки ІС з контактами смарт-карти (для контактної смарт-карти) та інкапсуляцію ІС в захисне покриття (як правило епоксидним).

• Виробництво карти

ІС поміщається у пластикову карту, і може мати печатку, тиснення, лист з магнітною смугою, та інші процеси "обробки", які застосовуються на даному етапі.

• Персоналізація та кастомізація

Перед видачею карта повинна бути підготовлена для її власника. Це означає підготовку початкових конфігурацій: завантажені усі програми, додатки, данні, які є індивідуальні для кожного власника, наприклад, ім'я власника картки та ПІН код та інше.

• Видача картки та її використання

На заключному етапі картка видається власнику (та супроводжуючі документи) та починає використовуватись у системі.

Кожен з етапів життєвого циклу виробництва піднімає питання безпечності кожного з етапів. У таблиці нижче представлені питання безпеки на кожному етапі (табл. 1).

5. МОДЕЛЬ ЗАГРОЗ

Напад визначається як спроба одного або декількох сторін, що беруть участь у транзакції обдурити. Ми розглянемо два класи нападників: учасників системи та порушників ззовні (аутсайдер).

Нападаючими з боку системи можуть бути власник картки, картка емітента, які намагаються обдурити власника терміналу і т.д.

Аутсайдером може бути той, хто вкрав картку: тимчасовий власник картки, котрий вкрав картку у законного власника, або той, хто замінює програмне забезпечення терміналу або апаратного забезпечення.

Мотиви для атаки діляться на кілька широких категорій. Першим і найбільш очевидним це фінансові крадіжки, у тому числі крадіжки грошей або кредитів, або крадіжці послуг, що реалізуються для широкої громадськості, такі як телефонні картки. Є також уособленні атаки, де карткова система є проміжною метою для отримання доступу до комп'ютерної системи або іншого пристрою контролю доступу. Наприклад, використання карти доступу, щоб увійти до конкретної комп'ютерної системи для ознайомлення з конференційною інформацією. Є напад на приватне життя, де одна сторона хоче більше інформації про іншу, ніж визначається протоколом. Нарешті, є атаки, коли зловмисник прагне до популярності.

6. ПРОТОКОЛИ ДЛЯ СМАРТ-КАРТ

Широке поширення смарт-карт (інтелектуальних карт) для різноманітних комерційних, цивільних і військових застосувань (кредитні карти, карти соціального страхування, карти доступу в приміщення, що охороняються, комп'ютерні паролі і ключі і так далі) вимагає забезпечення таких послуг безпеки, як ідентифікація, автентифікація таких карт і їх власників.

Ці послуги реалізуються за допомогою криптографічних протоколів, наприклад таких як,

Таблиця 1

Питання безпеки на кожному з етапів життєвого циклу смарт-карти

Етап життєвого циклу	Питання безпеки
Розробка вбудованого ПЗ	Випадкове або зловмисне спотворення/ модифікація: - Бібліотеки ПЗ; - Операційної системи; - Програми. Доступ до розробки програмного забезпечення також може допомогти зловмисникові розробляти атаки на випущені картки
ІС розробка	Недоліки або зміни, що можуть привести до вразливості; Доступ до проектних даних, які можуть бути використані для нападу
ІС Виробництво	Доступ до зразків у тестовому режимі – це може призвести до руйнуванню конфіденційності або/та цілісності вмісту ІС; Доступ до/модифікація у тестовому режимі перевірки достовірності даних (наприклад, ключі, паролі) – де результати випробувань захищені перевіркою на автентичність, у зловмисника є можливість отримати результати та змінити їх; Доступ до/модифікація даних ініціалізації (наприклад, ключів)
ІС пакування	Доступ до зразків у тестовому режимі
Виробництво картки	Доступ до зразків в тестовому режимі; Доступ до операційної системи/прикладного ПЗ на початкової стадії, перш ніж всі заходи безпеки будуть застосовані – це може дозволити зловмиснику прочитати конфіденційні дані, або внести зміни в конфігурацію карти; Доступ до сировини картки – це може допомогти зловмисникові зробити підробку для використання її у системі
Персоналізація і кастомізація	Доступ до даних ініціалізації (наприклад, до ключів, кредитних лімітів або інших параметрів схеми); Доступ до особистих даних власника
Видача картки та її використання	Доступ до даних під час доставки; Доступ до даних дає повноваження для оновлення параметрів карти (включаючи розблокування); Доступ до оновлень ОС, який може бути використаний для атаки; Створення оновлень для ОС, наприклад, для завантаження шкідливого коду; Диференційний аналіз живлення (DPA); Диференціальний аналіз помилок (DFA); Фізичні атаки на ІС.

протоколи простої та строгої автентифікації та протоколи з розголошенням нульових знань (далі ZK(zero knowledge) протоколи).

Однією з вразливостей протоколів простої автентифікації полягає в тому, що після того, як пред'явник передасть перевірнику свій пароль, перевірник може, використовуючи даний пароль та видати себе за видати себе за пред'явника. Більш захищеними є протоколами строгої автентифікації. Справа в тому, що *A*, відповідаючи на запити *B*, зобов'язаний продемонструвати знання секретного ключа, хай навіть і одноразово, при цьому передана інформація не може бути прямо використана *B*. Проте деяка її частина може допомогти *B* отримати додаткову інформацію про таємницю *A*. Наприклад , *B* має можливість так сформувати запити, щоб передані відповіді аналізувалися на предмет вмісту додаткової інформації[5].

ZK – протоколи (ISO/IEC 9798-5) були розроблені спеціально для вирішення даної проблеми. Цієї мети можна досягти за допомогою демонстрації знання секрету, проте перевірник повинен бути позбавлений можливості отримувати додаткову інформацію про секрет пред'явника. Якщо сформулювати цю думку в більш суворої формі, то ZK-протоколи дозволяють встановити істинність затвердження і при цьому не передавати будь-якої додаткової інформації про саме затвердження [5].

Однією із переваг таких протоколів є те, що вони можуть використовуватися для електронних цифрових підписів, якщо сторону *B* замінити криптографічно стійкою односпрямованою геш – функцією. Сторона *A* може сформулювати низку запитів, використовувати односпрямовану геш функцію як віртуальну строну *B* (яка довільним чином буде вимагати одну відповідь на кожен запит) та надавати ці відповіді. *B* якості аргументів геш – функції використовуються набір відповідей та запитів. Таким чином, ні відповідь, ні запит не можуть бути змінені без зміни підпису. Результат дії криптографічної односпрямованої геш – функції є цілком довільний і не передбачуваний. Приймаюча сторона обчислює значення геш – функції і перевіряє коректність відповідей на запити. Якщо перевірка пройдена, то підпис може вважатися правильною.

Прикладом такого протоколу є схема ЕЦП Шнорра:

Нехай p і q прості числа, такі, що p ділить q-1, нехай g належить до Z_p.

1) $g^q = 1 \bmod p$, g не дорівнює 1. У якості таємного ключа вибирається $x \in \{1, ..., q\text{-}1\}$. Відкритий ключ $y = g^{(-x)} \bmod p$.

2) *A* обирає випадкове число $k \in \{1, ..., q\text{-}1\}$ та обчислює $r = g^k \bmod p$;

3) *A* обчислює $e = h(r, m)$, де m – повідомлення, що підписується.

4) *A* обчислює $s = (k + ex) \bmod q$ та посилає повідомлення m з підписом (e,s) одержувачу B.

5) *B* обчислює $r' = g^s * y^e \bmod p$ та перевіряє, чи виповнюється рівність $e = h(r',m)$. Якщо так, то підпис вважається дійсною, якщо ні – відкидається.

Перевага схеми Шнорра перед відомою схемою Ель – Гамаля полягає в тому, що k вибирається з меншої множини (довжина k – порядку 140 бітів). Це підвищує ефективність обчислення

дискретних експонент. Крім того, варто зауважити, що використання в схемі Шнорра геш – функції при обчисленні *e* і приведення підпису *s* за модулем *q скорочують довжину підпису в порівнянні зі схемою Ель Гамаля. Довжина підпису – один з найважливіших показників ефективності схеми.*

З вище наведеного, можна зробити висновок, що ZK-протоколи можуть застосовуватися в системах з підвищеним вимогою до безпеки, наприклад в таких, які основані на смарт-картах, але їх застосування пред'являє жорсткі вимоги до обчислювальних здібностям і розміру пам'яті, що істотно підвищує вартість смарт-карт.

ВИСНОВОК

Вважається, що смарт-карти пропонують більше безпеки та конфіденційності, ніж інші види засобів зберігання інформації або виконання операцій. Крім того, додатки, які застосовуються з технологією смарт-карт ілюструють, що смарт-карти є одним з кращих рішень для забезпечення та підвищення безпеки і цілісності їх системи.

Крім того, більшість нападів на сьогоднішній день відносяться до 3 класу атак, що означає, що витрати, пов'язані з крахом системи набагато більші, ніж вартість самої системи. Так як розвиток технологій в наш час є досить швидким, виробники оновлюють та підвищують рівень безпеки їхньої продукції постійно. Тому, як тільки хакери знаходять способи взлому системи, проблеми можуть бути вирішені на новому поколінні технології безпеки [4].

Захист смарт-карт відбувається з початку життєвого циклу карт, це означає, що при відповідному контролі за процесом виробництва, можна виключити наявність закладок.

І, нарешті, до висновку, смарт-карти є внутрішньо безпечним пристроями. Це безпечне місце для зберігання цінної інформації, такої як закриті ключі, номери рахунків, і важливі особисті дані, такі як інформація біометрії, медична інформація. Смарт-карта є також безпечне місце для виконання автономних процесів, таких як генерування державних чи приватних ключів. Смарт-карта може бути елементом вирішення проблеми безпеки в сучасному світі.

Література

[1] *Bruce Schneier, Adam Shostack,* "Breaking Up Is Hard To: Do Modeling Security Threats for Smart Cards", Oct. 1999.

[2] *David Everett,* "Smart Card tutorial" (26 parts), Sept. 1992-Oct. 1994.

[3] *Istvan Zsolt Berta, Zoltan Adam Mann,* "Smart Cards-Present and future", Budapest University of Technology and Economic.

[4] *Горбенко Ю.І., Горбенко І.Д.* Інфраструктури відкритих ключів.ЕЦП. Теорія та практика:монографія.

[5] ISO/IEC 9798-5. Information technology. Security techniques. Part 5. Mechanisms using zero-knowledge techniques.

Надійшла до редколегії 24.05.2011

Заросилова Марина Геннадіївна, магістрант кафедри БІТ ХНУРЕ. Область наукових інтересів: дослідження технологій смарт-карт.

Бондаренко Михайло Федорович, член-кореспондент НАН України, Лауреат державної премії України, доктор технічних наук, професор, ректор Харківського національного университету радіоелектроніки.

УДК 004.087.5

Анализ технологии смарт-карт / М.Ф. Бондаренко, М.Г. Заросилова // Прикладная радиоэлектроника: науч.-техн. журнал. – 2011. Том 10. № 2. – С. 264–270.

На сегодняшний день смарт-карты играют большую роль в качестве «активных» устройств безопасности. Благодаря ее программирующей памяти и микрокомпьютеру, смарт-карты могут удовлетворить специфические потребности в среде, в которой она будет использоваться. Смарт-карты позволяют безопасную обработку и хранение конфиденциальных данных, таких как права пользователей и криптографические ключи, а также выполнение криптографических алгоритмов. Они являются безопасными маркерами, с помощью которых пользователь может быть идентифицирован и аутентифицирован компьютерной системой или сетью связи и наоборот. Эта статья знакомит с особенностями чип-карт, их жизненным циклом и стандартами, регулирующими их, моделью доверия и угроз.

Ключевые слова: смарт-карта, микросхема, модель угроз, модель доверия, жизненный цикл.

Табл. 01. Рис. 02. Библиогр.: 05 назв.

UDC 004.087.5

Analysis of smart card technology / M.F.Bondarenko, M.G. Zarosilova / Applied Radio Electronics: Sci. Journ. – 2011. Vol. 10. № 2. – P. 264–270.

At present smart cards play an increasing role as 'active' security devices. Due to its microcomputer and programmable memory, a smart card can satisfy specific needs of the environment it is used in. Smart cards allow the secure handling and storage of confidential data such as user privileges and cryptographic keys as well as the execution of cryptographic algorithms. They are secure tokens by means of which a user can be identified and authenticated by a computer system or communication network and vice versa. This paper introduces the features of smart cards, their life cycle and standards that govern them, trust and threats model.

Keywords: smart card, chip, threats model, trust model, lifecycle.

Tab. 1. Fig. 2. Ref.: 5 items.