УДК 004.5:004.9

О.В. Бакай, В.Б. Дудикевич, Ю.В. Лах
Національний університет “Львівська політехніка”,
кафедра захисту інформації

ОСОБЛИВОСТІ КРИПТОГРАФІЧНОГО ЗАХИСТУ ПЛАТІЖНИХ КАРТОК З МАГНІТНОЮ СМУГОЮ ВІДПОВІДНО ДО ВИМОГ СТАНДАРТУ PCI DSS

Розглянуто принципи роботи платіжних карток з магнітною смугою. Виділено основні вразливості цієї технології та подано вимоги і рекомендації щодо подолання цих уразливостей відповідно до сучасних стандартів безпеки.

Ключові слова: дані тримача картки, критичні аутентифікаційні дані, розподіл ключів, двостороння аутентифікація, шифрування.

The paper discusses operating principles of bank cards with magnetic stripes. The main problems of this technology were defined and recommendations for solving them according to the modern security and encryption standards were presented.

Key words: cardholder data, sensitive authentication data, key distribution, dual-sided authentication, encryption.

Вступ

Розвиток платіжних систем характеризується поступовим звуженням сфери використання готівки та паперових платіжних документів із переходом до нових платіжних інструментів і технологій платежів. Електронні гроші широко залучаються до обігу і стають важливим інструментом фінансової інфраструктури економічно розвинених країн, які намагаються звести до мінімуму кількість готівкових операцій і готівкової маси в обігу. Для цього застосовується ціла низка заходів, одним з яких є розрахунки за допомогою карткових платіжних систем, – як внутрішньодержавних, так і міжнародних.

Важливим кроком для досягнення поставленої мети в Україні стало створення системи електронних міжбанківських платежів, що дало змогу значно збільшити швидкість, якість і надійність виконання операцій, а також гарантувати безпеку і конфіденційність банківської інформації завдяки засобам багаторівневого програмно-апаратного контролю для відстеження проходження платежу і запобігання спробам несанкціонованого доступу.

Принцип роботи картки з магнітною смугою та вимоги до шифрування полів даних

У сфері грошового обігу пластикові картки є одним з прогресивних засобів організації безготівкових розрахунків. У системі безготівкових розрахунків вони становлять особливий клас засобів платежу, які можуть володіти якостями як дебетових, так і кредитних інструментів.

Магнітна картка – це пластикова картка, яка відповідає специфікаціям ISO, має на зворотному боці магнітну смугу з інформацією обсягом близько 100 байтів пам'яті, яка прочитується спеціальним зчитувальним пристроєм, та місце для підпису [1, 2]. Такі магнітні картки поширені в усьому світі як банківські кредитні та дебетові картки. Смуга може бути

виготовлена для різних потужностей магнітного поля, і за цим параметром розрізняють низько- (300 ерст) і високоерцитивні (до 4000 ерст) магнітні смуги. Для стандартних зчитувальних пристроїв (рідерів) магнітна смуга завширшки 12,7 мм (04 дюйми) розташована на відстані 4 мм від краю картки. Магнітна смуга картки має, як правило, три доріжки, на які записується інформація. На кожній доріжці можна закодувати символи, кількість і перелік яких подано в табл. 1.

Таблиця 1

Технічні характеристики доріжок

Доріжка	Кількість символів	Символи кодування
Перша доріжка	Максимум 76	Букви від A до Z, цифри від 0 до 9, а також! @ # $ & * + – = [];:, < > ^
Друга доріжка	Максимум 36	Цифри від 0 до 9 а також =;: < >
Третя доріжка	Максимум 104	Цифри від 0 до 9 а також =;: < >

У фінансовій сфері переважно використовують другу доріжку. На ній постійно зберігається інформація, яка містить номер картки або банківського поточного рахунку, ім'я та прізвище власника, термін закінчення дії картки (ця інформація, як правило, повинна збігатися з інформацією, яка розміщена на лицьовому боці картки). Важливим елементом цієї інформації є персональний ідентифікаційний номер (PIN). Цей номер (код) має бути відомий лише власнику картки.

Є два режими роботи з магнітними картками. В режимі on-line пристрій (торговий термінал, електронна каса, банкомат) зчитує інформацію з магнітної картки, яка каналами зв'язку передається в центр авторизації карток. У режимі off-line інформація про покупку, зроблену власником картки, нікуди не передається, а зберігається в торговому терміналі або електронній касі. Через певний проміжок часу термінал зв'язується з банком і передає всю інформацію на хост.

Дві з 12 обов’язкових вимог стандарту PCI DSS [3, 4] формулюють необхідність шифрування даних:

– забезпечення захисту даних тримачів карт в ході їх зберігання;

– забезпечення шифрування даних тримачів карт під час їх передавання загальнодоступними мережами.

До даних про тримача картки належать PAN (номер картки), ім’я тримача картки і термін дії картки. Критичні аутентифікаційні дані містять (але не обмежуються цим переліком): повний вміст магнітної смуги, доріжка 1, доріжка 2 магнітної смуги, контрольне значення картки CVV, CVV2 (card verification value) – код перевірки справжності картки системи Visa (CVC для MasterCard), контрольні значення PIN (PVV) та PIN/PIN block. Критичні аутентифікаційні дані не можуть бути використані для жодних цілей, окрім як для авторизації транзакції.

За таких умов шифрування пов’язують із забезпеченням таких цілей безпеки:

– обмеження циркуляції даних про тримачів карток та критичних аутентифікаційних даних у відкритому вигляді лише точками зашифрування і розшифрування;

Усі дані про тримачів карток і критичні аутентифікаційні дані мають шифруватися лише алгоритмами, що схвалені ANSI X9 або ISO (Наприклад AES, TDES).

Критичні аутентифікаційні дані не можуть зберігатися після авторизації навіть у зашифрованому вигляді відповідно до вимог PCI DSS.

– використовувати надійні рішення щодо управління ключами відповідно до міжнародних та регіональних стандартів;

Управління ключами має здійснюватися відповідно до стандартів ANS X9.24 (усі пункти) / ISO 11568 (усі пункти) або до їх аналогів. Всі ключі та їх компоненти мають генеруватися з

використанням схвалених процедур випадкового чи псевдовипадкового підбору, наприклад NIST 800-22. Документація, що описує процес установлення та функціонування системи управління ключами, має бути доступна та надана за запитом для її оцінювання та перевірки. Передавання ключів каналами зв'язку має бути захищено, наприклад за методом розподілу ключів, описаним в X9/TR-34 Interoperable Method for Distribution of Symmetric Keys Using Asymmetric Techniques, Part 1 – Using Factoring-Based Public Key Cryptography Unilateral Key Transport або еквівалентним методом.

Якщо використовується дистанційний розподіл ключів, то повинна здійснюватись двостороння аутентифікація пристроїв відправлення та отримання. Ключі, що використовуються безпосередньо в процесі шифрування поля даних, мають бути унікальними для кожного пристрою і використовуватись лише для шифрування даних про тримачів карт та критичних аутентифікаційних даних. Відповідно до PCI PIN Security Requirements ключі для шифрування PIN не можна використовувати для шифрування поля даних.

– використовувати довжини ключів та криптографічні алгоритми, що відповідають міжнародним та регіональним стандартам;

Ключі шифрування мають володіти стійкістю, еквівалентною стійкості як мінімум 112-бітного ключа. Еквівалентні стійкості для найбільш уживаних алгоритмів [5] наведено в табл. 2:

Таблиця 2

Еквівалентні стійкості для алгоритмів

Алгоритм	Довжина
TDES	112[1]
AES	128[2]
RSA	2048
ECC	224
SMA	224

– захистити пристрої, які виконують криптографічні операції від фізичної та логічної компрометації;

Пристрої, що виконують криптографічні операції, підлягають незалежному оцінюванню для гарантії того, що їх комплектуючі та програмне забезпечення є достатньо стійкими до атак.

Симетричні та закриті ключі мають бути захищені від фізичної та логічної компрометації, а відкриті ключі захищені від підміни із гарантованою цілісністю та достовірністю.

– для бізнес-процесів використовувати додаткові облікові записи чи ідентифікатор транзакції, які не використовують PAN після авторизації, наприклад, під час повторних платіжних операцій, підтримки програм лояльності клієнта чи управління інцидентами при шахрайстві.

Відповідність не є одноразовою вимогою. Торговельні підприємства повинні підтверджувати свій статус відповідності один раз на рік, але передбачено, що підтримка відповідності буде проводитися завжди.

Принципи побудови та вимоги до програмних засобів захисту

Програмними ЗЗІ називають спеціальні програми, що входять до складу програмного забезпечення АС для вирішення в них (самостійного чи в комплексі з іншими засобами) завдань захисту. Програмні ЗЗІ являють собою обов'язкову і важливу частину механізму захисту АС. Така їх роль визначається такими перевагами: універсальністю, гнучкістю, простотою реалізації, надійністю, можливістю модифікації і розвитку.

При цьому під універсальністю розуміють можливість вирішення програмними ЗЗІ багатьох завдань захисту.

Під надійністю розуміють високу програмну стійкість за великої тривалості неперервної роботи і відповідність високим вимогам і достовірності керівних впливів за наявності різних дестабілізуючих факторів. Програмні можливості зміни і розвитку програмних ЗЗІ визначаються самою їх природою.

Істотним недоліком програмних ЗЗІ є можливість їх реалізації лише в тих структурних елементах АС, де наявний процесор, хоча функції захисту можуть реалізовуватися, гарантуючи безпеку інших структурних елементів. Окрім цього, програмним ЗЗІ притаманні такі недоліки [6]:

- необхідність використання часу роботи процесора, що збільшує час відгуку на запити і, як наслідок, зменшує ефективність роботи;
- зменшення обсягу оперативної пам’яті і пам’яті на зовнішніх запам’ятовувальних пристроях, доступного для використання функціональними задачами;
- можливість випадкової чи навмисної зміни, внаслідок чого програми можуть не лише втратити здатність виконувати функції захисту, але і стати додатковим джерелом загрози безпеці;
- обмеженість через жорстку орієнтацію на архітектуру певних типів ЕОМ (навіть у межах одного класу) – залежність програми від особливостей базової системи введення/виведення, таблиці векторів переривання тощо.

Для організованої побудови програмних ЗЗІ характерною є тенденція розроблення комплексних програм, що виконують низку захисних функцій, причому найчастіше до цих функцій належать розпізнавання користувачів, розмежування доступу до масивів даних, заборона доступу до деяких областей оперативної пам’яті тощо. Переваги таких програм очевидні: кожна з них забезпечує вирішення деяких важливих завдань захисту.

З описаних недоліків та переваг випливають такі вимоги до формування програмних ЗЗІ: функціональна повнота, гнучкість і уніфікованість використання.

Аналіз показав, що якнайкраще вимоги гнучкості та уніфікованості задовольняють такі сукупності принципів: наскрізна модульна будова, повна структуризація, представлення машинно-незалежною мовою.

Принцип наскрізної модульної побудови полягає в тому, що кожна з програм будь-якого рівня та об’єму має представлятися у вигляді системи можливих модулів, причому кожний модуль будь-якого рівня має бути повністю автономним і мати стандартні вхід та вихід, що забезпечує компонування з будь-якими іншими модулями. Неважко помітити, що ці умови можуть бути виконані, якщо програмне забезпечення буде розроблятися за принципом “згори донизу”, тобто відповідно до принципу повної структуризації.

Представлення машинно-незалежною мовою передбачає, що представлення програмних модулів має бути таким, щоб їх з мінімальними зусиллями можна було ввести до складу програмного забезпечення будь-якої АС. Сьогодні алгоритмічні мови високого рівня повністю відповідають цим вимогам. (Такі мови часто є трансплатформеними та підтримуються такими середовищами, як MS CryptoAPI 2.0 та.NET Framework).

Висновки

Оскільки магнітний запис як найпоширеніший спосіб нанесення інформації на пластикову картку не забезпечує необхідного рівня захисту як від підробок, так і від розголошення інформації, записаної на магнітній смузі, шифрування полів даних стає критичним моментом в платіжних системах з магнітними картками.

Дотримання описаних вимог щодо шифрування покликане забезпечити досягнення поставлених цілей інформаційної безпеки у системах, що виконують еквайрингові операції: платіжні термінали, точки продажу торгово-сервісних підприємств, корпоративні сервери, сервери агрегування транзакцій, платіжні шлюзи, процесингові системи.

1. Пиріг С. О. Платіжні системи: навч. посібник. – К.: ЦУЛ, 2008. – 240 с. 2. Голдовский И. Безопасность платежей в интернете. – СПб.: Питер, 2001. 3. Рики Магалхаес PCI DSS Совместимость / Ricky M. Magalhaes // [Електронний ресурс]. http://www.win dowsecurity.com/articles, 2008. 4. Бакай О., Брич Т., Лах Ю. Технології захисту банківських міжнародних платіжних карток // Вісник Нац. ун-ту "Львівська політехніка" "Автоматика, вимірювання та керування". – 2012. – № 741. – С. 184–187. 5. Лучшие практики Visa по шифрованию полей данных, версия 1.0. [Електронний ресурс]. http://www.pcidss.ru/files/pub/pdf/visa_encryption_ best_practices_russian.pdf 6. Хорошко В., Чекатков А. Методы и средства защиты информации. – К.: Юниор, 2003. – 504 с.