УДК 621.3:004.056(0.43.2)

Захарчук Н.В., Бубенкова В.С.
Національний авіаційний університет, Київ

ЗАСТОСУВАННЯ КРИПТОГРАФІЇ ДЛЯ ПЛАТІЖНИХ КАРТОК З МАГНІТНОЮ СМУГОЮ

Вступ. Поширення банківських платіжних карток призвело до ризику втрати як цінної інформації, так і коштів клієнтів з боку шахраїв. У той час як вводяться інші, більш захищені методи шифрування, магнітна картка й досі є набагато дешевшою ніж інші альтернативи і сьогодні картки з магнітною смугою – найпоширеніший тип карт, що використовується в банківських системах.

Методи захисту платіжних магнітних карток поступово покращуються і при правильному застосуванні можуть надати відмінний захист для фінансових транзакцій при низькій собівартості виготовлення.

Мета дослідження – дослідити захищеність платіжних карток та методів криптографічного захисту.

Основна частина. Найпоширеніше використання криптографії в платіжних банківських картках – це забезпечення захисту ПІН (Персонального Ідентифікаційного Номера) картки та PIN-коду, що необхідний для використання магнітної картки в місцях, де не можна здійснити контроль за правомірністю доступу, наприклад в АТМ-банкоматах або в будь-яких інших ситуаціях, де здійснити звичайну операцію підпису чеку неможливо.

Другим найбільш поширеним методом використання криптографії є надання механізмів контролю за оригінальністю магнітної смуги картки.

Суть цього методу полягає в попередженні виготовлення карт шахрайським шляхом, коли на магнітну смугу записується значення, яке не може бути отримано з видимої або нанесеної на картку інформації. Коли карта перевіряється в режимі он-лайн, це значення може бути перевірено для того, щоб підтвердити справжність картки. Для цього існує кілька різних стандартів, найбільш використовувані це CVV (Visa Card Verification Value) або його аналог для Мастеркард – CVC. Комбінація статичних даних як, наприклад, номер рахунку тричі шифрується, використовуючи спеціальну пару ключів Card Verification. Вибрані з результату цифри використовуються для створення CVV і пишуться на магнітну смугу картки. CVV складається з декількох цифр, які шифруються потрійним шифруванням TripleDES, тому ключі CVV добре захищені і його наявність ще раз додатково підтверджує, що картка є справжньою.

Загроза підробки карток призвела до введення Card Verification Value, що унеможливлює отримати послідовності цифр, які записані на магнітній смузі, так як цифри створені процесом шифрування, а потім записані на магнітну смугу карти. Це означає що електронний збір інформації про транзакції АТМ-банкоматів або POS-терміналів ефективно захищений від шахраїв.

Висновок: Так як CVV просто додатковий метод захисту, він не може повністю захистити від шахрайського збору інформації з магнітних карток, наприклад, на фальшивих АТМ-банкоматах. Тому необхідно вдосконалювати криптографічні методи захисту платіжних карток клієнтів з метою зменшення шахрайств.

Науковий керівник – Ю.В.Пепа, к.т.н., доц.