Максим Шаповал
НТУУ «КПІ», ФТІ
УДК 004.77

МОДЕЛЬ ЗАХИЩЕНОЇ СИСТЕМИ ПЕРЕДАЧІ ДАНИХ POS ТЕРМІНАЛЬНОГО ТРАФІКУ

Анотація: **Наведені недоліки існуючих методів передачі даних між процесинговим центром та платіжними POS терміналами. Запропонована модель захищеної системи передачі даних базується на аналізі можливих варіантів мінімізації існуючих загроз, усуненні існуючих недоліків та виборі найоптимальнішого варіанту. Наведено узагальнюючий опис моделі передачі даних POS трафіку, що не матиме недоліків існуючих систем.**
Summary: **In this article noted breaches of existing methods of data transfer between processing center and payment POS terminal. And proposed model of secure data transmission system based on the analysis of possible options to minimize existing threats and eliminate existing breaches and choosing the best option. Conclusion of article is generalized description of the model data POS traffic will have drawbacks of existing systems.**
Ключлві слова: **POS термінал, передача даних, процесинговий центр, банківська таємниця, PCI DSS**

I Вступ

У [1] розглянуті існуючі на сьогоднійній день методи захисту даних трафіку, що проходить між POS-терміналами та Процесинговим центром:

- відкрита передача даних;
- централізований збір даних у торговельному відділенні та їх шифрована передача;
- побудова шифрованого IPSec тунелю від Банку до кожного POS-терміналу;
- передача даних по захищеному приватному шифрованному з'єднанню;
- передача даних з використанням протоколу рівня захищених сокетів (SSL).

Проведено аналіз переваг і недоліків існуючих методів та визначені недоліки, що притаманні всім методам. Усі методи не гарантують повної безпеки процесу обміну даними між POS-терміналами та Банком, а саме:

- забезпечення доступності і надійності каналів зв‘язку між Хостом та POS-терміналами;
- двобічна авторизація (Хосту та POS-терміналів)

1. Вимоги PCI DSS в частині реалізації SSL **[2]**

До складу нормативної документації PCI входить Керівництво з реалізації SSL для POS-терміналів, в якому перераховані наступні вимоги:

- обов'язкова двостороння автентифікація за стандартом SSL;
- заборона використання алгоритму MD5 для перевірки підписів сертифікатів;
- заборона використання ключів RSA довжиною менше 1024 біт;
- POS-термінал повинен підтримувати хоча б один шифронабір (Cipher Suite) зі списку дозволених для PCI;
- Заборона використання SSL v2.0.

Найбільш істотною вимогою є двостороння автентифікація терміналу і хостового сервера саме по протоколу SSL. Тим самим заборонена практика часткового використання SSL, популярна в HTTP-додатках, коли для автентифікації сервера застосовується наявний у клієнта сертифікат, а для автентифікації клієнта - безпосередня відправка пароля на сервер. Автентифікація клієнта по протоколу SSL вимагає наявності у терміналу файлу сертифіката в комплекті з секретним ключем, який може бути завантажений в термінал до інсталяції, аналогічно завантаженню майстер-ключа ПІН-пада. Проте, як нам відомо, сертифікати мають обмежений термін життя, тому постає задача завантаження нових сертифікатів у POS-термінали [3, 4].

Варіант прямого доступу до POS-терміналів можна виключити, адже необхідно буде задіяти величезну кількість ресурсів для виїзду та обслуговування POS-терміналів.

Постає головна задача – необхідно грамотно організувати та обслуговувати інфраструктуру відкритих ключів (PKI, Public Key Infrastructure).

Проблема полягає в тому, що потрібно здійснювати неперервний контроль за багатьма розподіленими системами (касові апарати, банківські термінали, сервери ЦОД і т. д.), які знаходяться за межами Банку і, крім того, можуть використовуватися і обслуговуватися третіми сторонами або просто до них є фізичний

доступ сторонніх осіб. При цьому додатки контролю повинні бути компактними, керованими і не впливати на продуктивність додатків.

II Модель захищеної передачі даних між POS-терміналом та процесингом

1. Забезпечення доступності

Для забезпечення наступрості Хосту та POS терміналів доцільно використовувати технологію MPLS, котра забезпечить надійність каналу зв‘язку.

В основі MPLS лежить принцип обміну міток. Любий пакет, що передається, асоціюється з тим чи іншим класом мережевого рівня (FEC), кожний з яких ідентифікується визначеною міткою. Значення мітки унікально тільки для ділянки маршруту між сусідніми вузлами мережі MPLS, які мають назву маршрутизаторів з комутацією міток (LSR). Мітка передається у складі будь-якого пакета. При цьому спосіб її прив’язки до пакету залежить від технології, що використовується на канальному рівні.

Вся операція потребує тільки одноразової ідентифікації значення полів в одному рядку таблиці. Це займає менше часу, ніж порівняння IP-адреси відправника з найбільш довшим адресним префіксом у таблиці маршрутизації, яке використовується при традиційній маршрутизації.

2. Пошук оптимального криптографічного алгоритму для шифрування даних POS-термінального трафіку

Для побудови системи захисту даних POS-термінального трафіку однією з ключових задач є визначення оптимального алгоритму шифрування даних, який матиме функціональний компроміс між швидкістю роботи та криптостійкістю. Враховуючи особливості використання систем карткового бізнесу пріоритизація швидкості та криптостійкості є неперервним процесом.

Як видно із наведеної вище криптостійкості алгоритмом для шифрування даних, що передаються, доцільніше використовувати симетричні алгоритми, бо в асиметричних алгоритмах необхідно застосовувати довгі ключі (512 бітів і більше). Довгий ключ різко збільшує час шифрування. Крім того, генерація ключів вельми тривала. У симетричних алгоритмах використовують більш короткі ключі, що забезпечує швидке шифрування.

Проте для розподілу ключів необхідно використовувати асиметричні алгоритми, оскільки дані між POS-терміналом та процесингом передаються відкритими каналами провайдерів (у незахищених каналах).

Тому при проектуванні захищеної системи доцільно застосовувати і симетрічі, і асиметрічні алгоритми. За допомогою асиметричних розсилати ключі, симетричними же – шифрувати передавану інформацію.

Зауважу, що в урядових і військових системах зв'язку використовують лише симетричні алгоритми, бо немає строгого математичного обгрунтування стійкості систем з відкритими ключами, як, втім, не доведено і зворотнє [5, 6].

2.1. Пошук оптимального симетричного алгоритму

Враховуючи показники найчастіше використовуваних в Україні POS-терміналів до розгляду доцільно взяти наступні алгоритми:

- DES
- 3DES
- AES

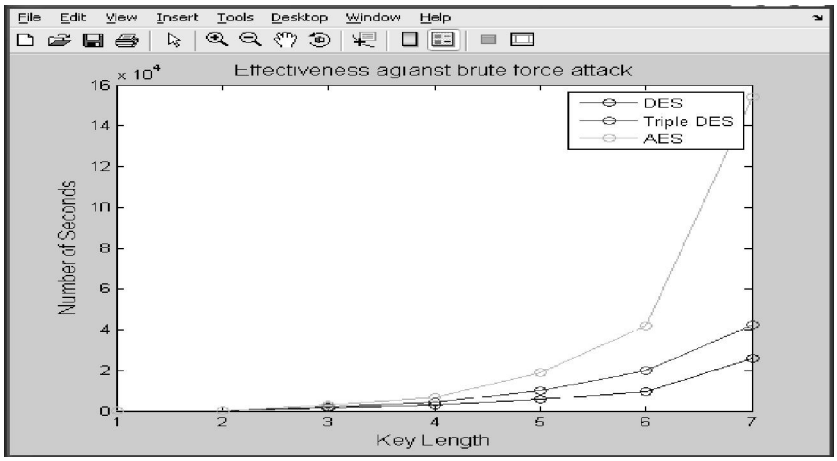

Рисунок 1 – Порівняння швидкості грубого розшифрування симетричних алгоритмів залежно від довжини ключа шифрування

* При використанні обладнаня з технічними характеристиками, що близькі до технічних показників POS-терміналів (Процесор (криптопроцесор) – ARM 7, Пам'ять - 16 Mb) швидкість обробки даних може змінитися.

Судячи з результатів, що проілюстровані на рис. 1, можна зроити висновок, що для даних POS-термінального трафіку доцільно використовувати алгоритм шифрування – **AES**.

2.2. Пошук оптимального алгоритму розподілу ключів шифрування

Враховуючи той факт, що швидкість обслуговування клієнтів сервісами POS-терміналів відіграє вкрай важливу роль, можна зробити висновок, що для розподілу ключів слід використовувати алгоритм RSA.

3. Розподіл сертифікатів

Згідно з вимогами PCI DSS необхідна двостороння автентифікаця учасників SSL з'єднання. Отже SSL концентратор, що знаходиться в процесингу банку, та кожен з POS терміналів мають бути учасниками одного центру сертифікації та мати сертифікати [2].

Якщо запис сертифікату на SSL концентратор не викликає питань та складності, то процес запису сертифікатів на POS термінал може викликати складності, до того ж не технічні, а організаційно-нормативні. Розглянемо можливі варіанти.

Для повної ідентифікації учасників SSL з'єднання достатньо завантажити один сертифікат [5].

3.1. Використання єдиного сертифікату для всіх POS-терміналів

Для повної ідентифікації учасників SSL з'єднання достатньо випустити лише два сертифікати: один сертифікат завантажити на SSL концентратор, а другий сертифікат – на кожен POS-термінал мережі Банку.

Недоліки даного способу:

При компрометації одного сертифікату (котрий встановлюється на POS-термінали), дані зі всіх POS-терміналів можуть бути скромпрометовані.

3.2. Використання унікального сертифікату для кожного з POS-терміналів

Наступний способ полягає у тому, щоб випускати сертифікат для кожного учасника центру сетрифікації (рис. 2).

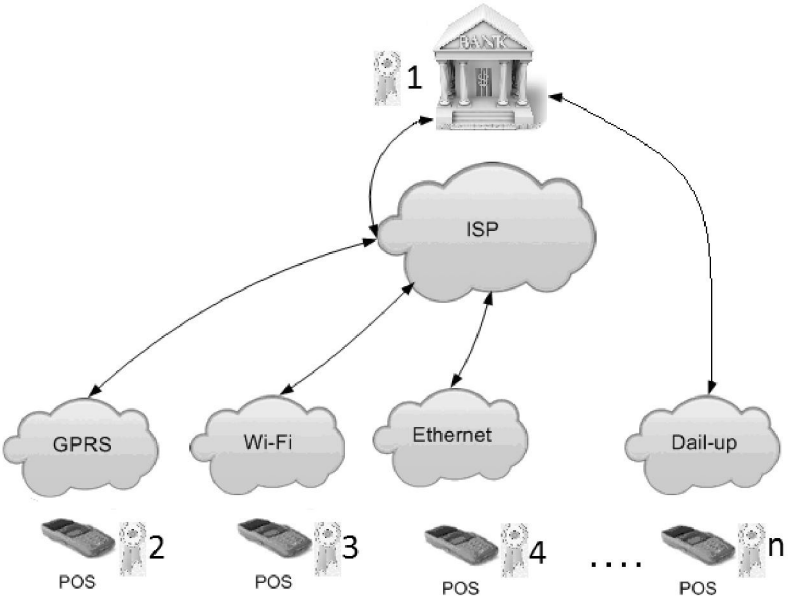

Рисунок 2 – Використання унікального сертифікату для кожного з POS-терміналів

Даний спосіб дозволяє однозначно ідентифікувати кожного з учасників POS-термінальної мережі. При компрометації сертифікату одного з POS-терміналів всі інші залишаються працездатними та захищеними.

Зазначу, що для завантаженя сертифікату, обліку відповідності сертифікату – POS-терміналу та контролю строку дії кожного з сертифікатів збільшується навантаження трудозатрат, але враховуючи переваги в захищеності POS-термінальної мережі, дані затрати виправдані.

3.3.1. Перше завантаження сертифікатів

Визначивши кількість учасників центру сертифікації, необхідно власне завантажити сертифікати до кожного з POS-терміналів та SSL-концентратора. Завантаження доцільно виконувати, маючи прямий доступ до кожного із учасників центру сертифікації, адже при віддаленому завантаженні може бути використана атака «людина посередині» [1].

Завантаження сертифікату рекомендується виконувати компонентним способом, аби виключити людський фактор (підміну, чи крадіжку сертифікату для подальшого зловмисного використання).

Компонентний спосіб полягає в тому, щоб розділити сертифікат на три частини, кожну з яких індивідуально записуватиме окрема людина (рис. 3).

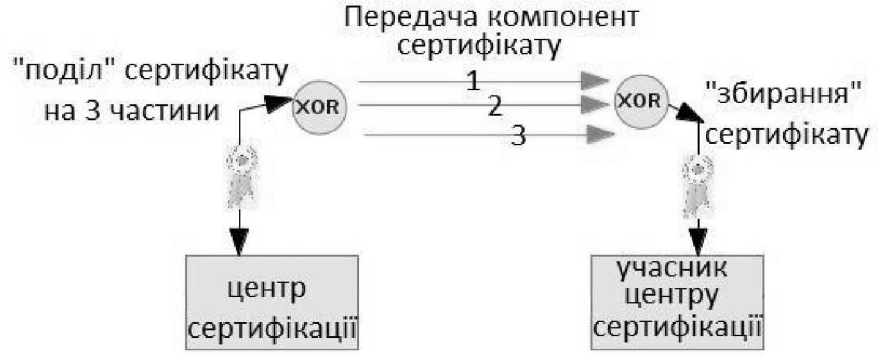

Рисунок 3 – Компонентна передача сертифікату

XOR — логічна операція, що приймає значення «істина» тоді, і тільки тоді, коли значення «істина» має рівно один з її операндів. У випадку двох змінних результат виконання операції є істинним тоді і тільки тоді, коли лише один з аргументів є істинним. Для функції трьох і більше змінних результат виконання операції буде істинним тільки тоді, коли аргументів, рівних 1, на заданому наборі буде непарна кількість. Така операція природним чином виникає в кільці відрахувань по модулю 2, звідки і походить назва операції.

Операція XOR є асоціативною, комунікативною та дистрибутивною, а отже порядок вводу компонентів сертифікату не є важливим. Також зрозумілим є той факт, що при втраті чи пошкодженні одного з компонентів сертифікату, його відновлення стає неможливим.

3.3.2. Планова заміна сертифікатів

Подальша заміна сертифікатів можлива і при віддаленому доступі до POS-терміналів, адже вони вже є ідентифікованими. Відстеження строку валідності сертифікату є задачею ценру сертифікації та реалізовано майже в усіх центрах сертифікації. Проте заміна великої кількості сертифікатів на віддалених ділянках є досить кропіткою задачею. Як відомо з досвіду, для генерації одного сертифікату та його завантаження необхідно близько п’яти хвилин. Враховуючи той факт, що кількість POS-терміналів налічується тисячами, зрозумілим стає той факт, що модель подальшого завантаження сертифікатів потребує додаткового покращення.

Як відомо, POS-термінали в більшості випадків підключаються невеличкими групами у торговельних точках, а отже постає необхідність одночасної заміни сертифікатів на всіх POS-терміналах однієї, або декількох торговельних точках. Саме для задач групової заміни сертифікатів створені комплески групового розподілу сертифікатів. Дані комплекси дозволяють генерувати ключі не індивідуально для кожного пристрою, а цілими списками з унікальними ідентифікаторами пристроїв. Уже отримані сертифікати необхідно завантажити на POS-термінали за допомогою спеціалізованого програмного забезпечення, що створюється виробниками, чи компаніями, що обслуговують POS-термінали.

III Узагальнюючий опис моделі захисту даних POS-термінального трафіку

Підсумовуючи інформацію, отриману в попередніх розділах, загальну модель та вимоги до системи захисту даних POS-термінального трафіку слід представити так, як показано на рис. 4.

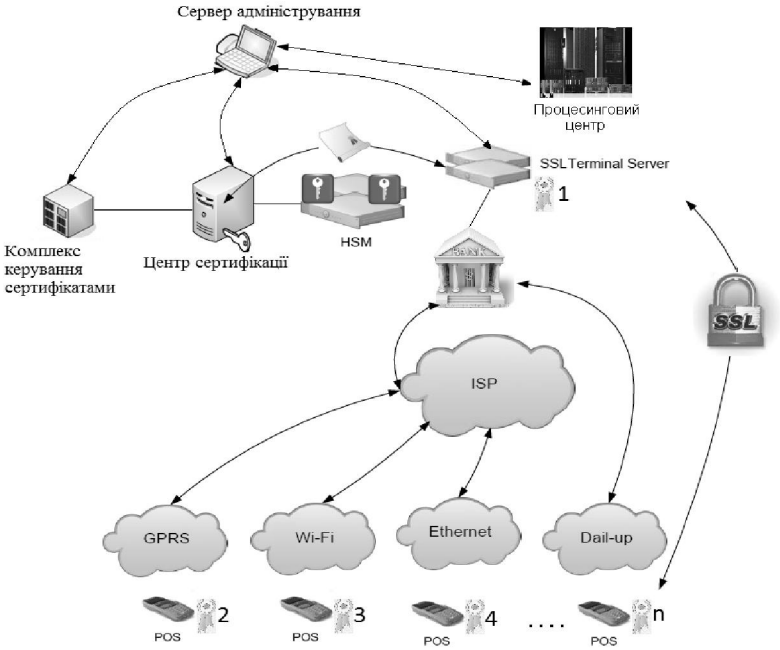

Рисунок 4 – Модель захищеної мережі POS-термінального трафіку

Мережа POS-терміналів має складатися з наступних елементів:

- комплекс POS-терміналів;
- центр цифрових-сертифікатів;
- модулі безпеки HSM;
- процесинг Банку;
- комплекс керування сертифікатами;
- SSL-концентратор;
- сервер адміністрування POS-термінальною мережею;
- локальна обчислювальна мережа Банку;
- мережа інтернет-провайдеру із наданням сервісу IP MPLS.

Першочерговою задачею є випуск сертифікатів за запис їх компонентним способом у SSL-концентратор та кожен із POS-терміналів. Кожен сертифікат створюється в HSM модулі та підписується кореневим сертифікатом, що зберігається у HSM модулі. Сертифікати для POS-терміналів створюються за допомогою комплексу групових сертифікатів. Максимальний строк життя цифрових сертифікатів – 1 рік. Подальша заміна сертифікатів на POS-терміналах відбувається через випуск групи сертифікатів на комплексі керування сертифікатами, а їх запис відбувається через віддалений доступ, використовуючи програмне забезпечення фірм–розробників продуктів для POS-терміналів.

Обмін данними між POS-терміналом та Банком виконується лише у шифрованому вигляді. Для шифрування використовується протокол SSL. SSL тунель будується за двосторонньою автентифікацією (клієнта та сервера). Як автентифікатори виступають записані раніше цифрові сертифікати. Дані шифруються за допомогою алгоритму AES з ключем шифрування 256 bit. Розподіл ключів шифрування виконується за алгоритмом RSA з ключем 1024 bit.

Після обміну шифрованими даними, отримана інформація (номер картки, PIN код, сумма зняття та ін) потрапляє до процесингу Банку, де перевіряється банківські дані даної картки.

Слід зазначити, що дана модель може бути доповнена банкоматами та терміналами миттєвих платежів.

IV Висновок

В статті наведені недоліки існуючих методів передачі даних від POS терміналів, а саме забезпечення доступності сервісу та авторизація й довірчість кожного з учасників процесу. Для цих недоліків запропоновані варіанти їхнього усунення з порівняльним аналізом кожного варіанту. Для усунення недоліку доступності сервісу запропоновано використання механізму MPLS, а для усунення недоліку авторизації

кожного учасника процесу запропоновано використання системи сертифікації з унікальним сертифікатом для кожного POS терміналу.

Підрахунок ризиків щодо використання кожного методу передачі даних від POS терміналу до процесингу, згідно з рекомендаціями Національного Банку України, буде завданням наступного дослідження.

Список використаної літератури: ***1.*** *Alan G. Konheim Computer security and cryptography / Alan G. Konheim - John Wiley & Sons, Inc., 2007 - p. 542.* ***2.*** *PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) Version 3.0 is active from January 1, 2014.* ***3.*** *К. Г. Явлинский «Динамическая модель банковской сети» / Кирилл Григорьевич Явлинский – 2-е издание, исправленное и дополненное -из-во ДМК Фин., 2013 – 480 с.* ***4.*** *СОУ Н НБУ 65.1 СУІБ 1.0:2010 МЕТОДИ ЗАХИСТУ В БАНКІВСЬКІЙ ДІЯЛЬНОСТІ. СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ. ВИМОГИ (ISO/IEC 27001:2005, mod)* ***5.*** *Carlisle Adams Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations / Carlisle Adams, Steve Lloyd, Macmillan Technical Publishing 1999 – p. 296.* ***6.*** *Збірник наукових праць "Спеціальні телекомунікаційні системи та захист інформації" випуск 2(26) 2014 с.87-97 Шаповал М. В. Порівняльний аналіз методів захисту даних pos-термінального трафіку*

Юрій Васильєв
ДержНДІ Спецзв'язку

УДК 004.056

КЛАСИФІКАЦІЯ ТА АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ В КЛЮЧОВИХ СИСТЕМАХ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Анотація: **Наведено класифікацію загроз інформаційній безпеці систем управління ключових систем інформаційної інфраструктури та методи їх аналізу.**
Summary: **The classification and methods of analysis of threats to information security management systems key of information infrastructure systems.**
Ключові слова: **Загрози, інформація, інформаційна безпека, ключові системи інформаційної інфраструктури**

І Вступ

Більшість сучасних систем управління (СУ) ключовими системами інформаційної інфраструктури (КСІІ) являє собою територіально розподілені системи, які взаємодіють між собою даними (ресурсами) та управлінням (подіями) локальних обчислювальних мереж (ЛОМ) та окремих ЕОМ.

У розподілених СУ КСІІ можливі всі характерні для локально розташованих (централізованих) обчислювальних систем способи несанкціонованого втручання в їх роботу і доступу до інформації, що обробляється. Крім того, для них є і специфічні канали вторгнення в систему і несанкціонованого доступу до інформації, наявність яких пояснюється низкою їх особливостей.

Основні особливості розподілених СУ КСІІ:

територіальна розподіленність компонентів СУ і наявність інтенсивного обміну інформацією між ними;

широкий спектр способів подання, зберігання і протоколів передачі інформації, що використовуються;

інтеграція даних різного призначення, що належать різним суб'єктам, в рамках єдиних баз даних і, навпаки, розміщення необхідних деяким суб'єктам даних у різних віддалених вузлах (базах даних) мережі;

відокремлення власників даних від фізичних структур і місця розміщення даних;

використання режимів розподіленої обробки даних;

участь у процесі автоматизованої обробки інформації великої кількості користувачів і персоналу різних категорій;

безпосередній і одночасний доступ до ресурсів (в тому числі і інформаційних) великого числа користувачів (суб'єктів) різних категорій;

високий ступінь різнорідності задіяних засобів обчислювальної техніки і зв'язку, а також їх програмного забезпечення;

відсутність спеціальних засобів захисту в більшості типів технічних засобів, які використовуються в СУ КСІІ.