Стаття подана в *Інформаційному бюлетені з міжнародної стандартизації 3-2011*

Стандарти у сфері платежів і, зокрема, стандарти у сфері безпеки платежів, є наріжним каменем системи роздрібних платежів. Технічний комітет ***ISO/TC 68 "Фінансові послуги"*** розробляє стандарти, які є важливими для забезпечення миттєвого виконання мільярдів транзакцій на трильйони доларів.

Без стандартів ISO та платіжних систем, розроблених відповідно до вимог цих стандартів, власник картки з Кігалі, Руанда, не зможе швидко, зручно і безпечно оплачувати товари та послуги під час поїздки до Парамарібо, Сурінам. Більш того, без стандартів ISO в галузі безпеки фінансові установи з усього світу не змогли б побудувати глобальну систему співробітництва та багатомільярдну платіжну систему за допомогою карток.

Багато стандартів ISO в сфері безпеки роздрібних фінансових платежів зосереджують увагу на захисті персонального ідентифікаційного номеру (PIN), який підтверджує право людини використовувати конкретну платіжну картку. PIN-код, який є досить коротким для легкого запам'ятовування, в результаті може бути легко викраденим, якби не цілий ряд вимог до кодифікування та заходів безпеки, встановлених стандартами ISO. Стандарти охоплюють вимоги до:

-

пристроїв обробляння та приймання PIN-кодів;

-

логічного захисту PIN-кодів за допомогою шифрування;

-

управління ключами шифрування для захисту PIN-кодів;

-

ідентифікації повідомлення про операцію з метою підтвердження її автентичності та цілісності;

-

форматів повідомлень та протоколів повідомлень про операцію.

Проти усіх загроз безпеці

Враховуючи швидкий розвиток платіжних систем та загроз їхній безпеці у стандартах ISO передбачається можливість постійного перегляду та оновлення вимог. У теперішній час зусилля спрямовані на з'ясування нових сценаріїв атаки, які досліджуються теоретично, а також на деяких випадках, які трапляються у реальному світі.

Сьогодні існують нові, більш досконалі алгоритми шифрування, однак їхнє впровадження не є простим відключенням старих і підключенням замість них нових алгоритмів шифрування. Навпаки, повинні бути ретельно розглянуті та проаналізовані вимоги безпеки та функціонального призначення з метою забезпечення впевненості у тому, що новий алгоритм повністю забезпечить очікування користувачів та усуне будь-які випадковості.

Однією з ілюстрацій того, наскільки важливі ці зусилля, є досвід останнього переведення галузі з старого на нові алгоритми шифрування, який відбувався 10 років тому. На ранній

стадії впровадження нових алгоритмів шифрування вони були майже в 36 (360000000 00000000) квадрильйонів разів менш ефективними, ніж планувалося. Завдяки змінам, що були прийняті за допомогою стандартизації та спрямовані на усунення недоліків і безпечне впровадження, нові алгоритми шифрування сьогодні ефективно працюють.

PIN-коди є статичними показниками, а тому повинні бути захищені скрізь, де вони використовуються, обробляються або зберігаються. Оскільки PIN-коди піддаються ризикам шахрайства, платіжний бізнес шукає нові методи ідентифікації, які встановлюють автентичність не через незмінні показники, а використовуючи ідентифікаційні коди, що динамічно генеруються і можуть бути використані тільки для однієї транзакції, що зменшить вірогідність шахрайств.

Нові можливості платежів

Безпека роздрібних платежів стосується не тільки PIN-кодів. У нашому надзвичайно взаємозалежному світі загроза безпеці існує фактично скрізь, оскільки метою кримінального розуму є робити гроші будь-яким способом. Таким чином, хоча використання і захист PIN-кодів залишається важливою темою для існуючих та нових стандартів ISO, разом з ними розробляються стандарти для вирішення проблем торгівлі та шахрайства.

Велика частина цієї роботи залишається для попередньої стандартизації, але технічні звіти ISO (TRs) є настановами для розроблення нових технологій. Наприклад, був розроблений технічний звіт ISO TR на визнання PIN-кодів для відкритих мережевих трансакцій, таких як електронна комерція в Internet.

Захист PIN-кодів у відкритому мережевому оточенні є серйозною проблемою, оскільки до мережі Internet підключені сотні мільйонів пристроїв. Відповідні настанови ISO щодо безпечного прийняття в цьому просторі попереджають, що PIN-коди ніколи не повинні бути введені в пристрої загального призначення для передачі через Internet. Якщо PIN-коди будуть використовуватися в цьому середовищі, то вони повинні використовуватись виключно у поєднанні з картами на інтегральній схемі (ICCs) і відправлятися на карту для перевірки.

Основою для розроблення сучасних стандартів на фінансові повідомлення є стандарт ISO 8583 на процеси передачі та формат фінансових повідомлень систем обробляння даних платіжних карт 20-річної давнини. Розроблення універсальних стандартів на обмін фінансовими повідомленнями є складним і трудомістким процесом, під час реалізації якого можуть виникнути різні проблеми. Дуже важливо, щоб у розробленні стандарту брали участь фахівці, відповідальні за різні напрямки розвитку фінансових операцій, які є майбутніми користувачами стандарту, оскільки стандарт буде сприяти безпечності проведення трансакцій.

Головною причиною збоїв у протоколах безпеки є існуючі проблеми взаємодії, що впливають на ефективність роботи, а тому під час розроблення цієї нової структури платежів необхідно враховувати вимоги всіх зацікавлених сторін.

Існує жарт, що найбільшою перевагою стандартів є те, що їх дуже багато, щоб зробити вибір. Справді, іноді може здатися, що це саме так. Але стандарти повинні відповідати потребам тієї конкретної галузі, для якої вони були розроблені. Це може призвести до розроблення багатьох стандартів, які стосуються однієї теми або декількох, але дуже близьких тем.

Прикладом цього є стандарт ISO/IEC на безпеку в галузі IT та аналогічні стандарти, розроблені технічним підкомітетом ISO/TC 68/SC 2. Стандарти ISO/IEC на безпеку IT забезпечують широкий, узагальнений набір вимог безпеки для IT-систем. В той же час стандарти, розроблені технічним комітетом ISO/TC 68, у багатьох випадках мають посилання на ці стандарти безпеки, при цьому не існує і не повинні розроблятись стандарти ISO/IEC IT для конкретних потреб ринку фінансових послуг.

Велика кількість вимог безпеки, які є необхідними для фінансового світу, будуть розглядатися як “надто зайві” в світі IT-середовища. Таким чином, впровадження стандартів ISO/IEC на безпеку у сфері IT часто буває недостатнім для захисту фінансових транзакцій.

Задоволення потреб клієнтів

Стандарти на безпеку, розроблені технічним комітетом ISO/TC 68, мають вирішальне

значення для торгівлі у 21 столітті. Сучасні процеси стандартизації забезпечують розгляд потреб усіх зацікавлених сторін, а в результаті стандарти забезпечать функціональність та безпеку, яких вимагає нинішній світ. Метою процесу стандартизації є своєчасність розроблення стандартів та їхня актуальність у мінливому світі.

Не всі нові технології повинні бути стандартизовані, а іноді просто занадто рано розробляти стандарти для нових технологій. У таких випадках більш доцільними виявляються технічні звіти та/або технічні умови ISO. Технологія або ж бізнес-структура повинна визріти до стандартів ISO.

Індустрія роздрібних фінансових платежів, це значний замовник і учасник розроблення стандартів і технічних звітів ISO. Ці документи, засновані на консенсусі, забезпечують щорічне проведення мільярдів транзакцій та оборот трильйонів доларів у торгівлі.

Джон Ф. Шітс, ISO Focus +