

УДК 004.6

А. Блавицький, С. Мацюк, С. Криськова

(Тернопільський національний технічний університет імені Івана Пулюя)

ОЦІНКА РОЗВИТКУ БЕЗПЕКИ ОПЛАТИ ПЛАТІЖНИМИ КАРТКАМИ

UDC 004.6

A. Blavitskyi, S. Matsiuk, S. Kryskova

ASSESSMENT OF THE SECURITY DEVELOPMENT OF PAYMENT CARDS

Навіть сьогодні в операціях з платіжними картками все ще використовуються застарілі технології. Щоб вирішити цю ситуацію, важливо проаналізувати та оцінити розвиток безпеки в методах електронних платежів, щоб зрозуміти, як захист даних, що використовуються в платіжних транзакціях, покращився з появою нових технологій.

Аналіз структурних елементів платіжної картки виявив десять елементів. Кожен із цих елементів, крім двох, реалізує функцію захисту платіжної картки. Першим винятком є магнітна смуга, яка є застарілою та незахищеною технологією для каналу наявної картки, яка все ще використовується, щоб зробити платіжну картку зворотною сумісністю із застарілими POI.

Другим винятком є CVV2, який є механізмом безпеки для каналу відсутності картки, який лише підтверджує володіння платіжною карткою.

Вивчення життєвого циклу платежу карткою виявило щонайменше п'ять суб'єктів, які відіграють певну роль у платіжному процесі. Для процесу оплати карткою доступні два платіжні канали: канал наявності картки та канал відсутності картки. Ці канали вказують на присутність або відсутність власника картки на об'єктах продавця, коли ініціюється оплата карткою.

Було розглянуто три технології EMVCo: чіп EMV, EMV 3DS 2.0 і токенизація платежів EMV. Кожна з цих технологій реалізує кілька функцій безпеки, включаючи автентифікацію даних, методи перевірки власника картки, потоки автентифікації, а також методи перевірки та ідентифікації. Ці функції безпеки є важливими, оскільки їх наявність, відсутність або поєднання впливає на загальну безпеку технології.

Дослідження стосувалося чотирьох стандартів PCI SSC: PCI DSS, PCI PTS, PCI PA-DSS і PCI P2PE. Головною метою цих стандартів є захист конфіденційних даних власника картки.

В майбутньому важливо продовжити детальне вивчення нових механізмів безпеки, які впроваджуються для інноваційних та альтернативних методів електронних платежів. Крім того, постійні дослідження та інновації в механізмах автентифікації покращать безпеку платежів карткою для обох платіжних каналів. Зазначимо, що постійна еволюція злочинних атак на електронні платежі з метою отримання незаконної вигоди повинна супроводжуватися та протистояти розробка нових технологій та заходів безпеки.

Література

1. «Payment Card Industry 3-D Secure (PIC 3DS) – Security Requirements and Assessment Procedures for EMV 3-D Secure SDK,» PCI Security Standard Council. [Online]. URL: <https://bit.ly/2xPLm5R> (Accessed: Nov. 10, 2022).