АЛГОРИТМЫ И МЕТОДЫ УПРАВЛЕНИЯ ПЛАТЕЖНЫМ АГРЕГАТОРОМ

Оберемко М. И.
Кафедра информационных технологий автоматизированных систем,
Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: oberemko.maxim@gmail.com

В данной работе рассматривается применение протокола 3-D Secure, в качестве эффективного метода управления безопасностью платежного агрегатора при проведении онлайн операций с кредитными и дебетовыми картами.

Введение

Основополагающим принципом в работе платежного агрегатора является безопасность и целостность персональных данных при проведении онлайн-платежей. В качестве ключевого и незаменимого метода управления безопастностью следует применять протокол 3D Secure (Three Domain Secure). Протокол основан на принципе верификации подлинности через 3 домена. Первый домен – домен банка-эмитена, который выпустил карту, используемую в операции. Второй домен – домен банка-эквайера, который принимает денежные средства. Третий домен – домен совместимости, который представляет собой инфраструктуру, предоставляемую платежной системой при проведении онлайн-платежа.

Кроме обеспечения дополнительного уровня защиты от мошенничества, в случае использования 3D Secure происходит «Перенос ответственности» за мошеннический платеж, при котором вся ответственность переходит от продавца к банку-эмитенту, выпустившему карту. Данное преимущество использования протокола позволяет бизнесу провысить конверсию.

I. Алгоритм управления протоколом 3D Secure 1.0

В настоящее время подавляющее большинство банков и платежных систем используют версию 1.0.2 при проведении онлайн CNP-платежей (Card Not Present), запрашивающих OTP-код (One Time Password). Данный протокол разработан на основе XML.

При инициализации транзакции в системе платежного агрегатора запускается алгоритм. В первую очередь осуществляется CRReq-запрос (Card Range Request). Данный запрос необходим, чтобы найти банк-эмитент проверяемой карты и получить CRR из домена взаимодействия. Следующим шагом агрегатор отправляет VeReq-запрос (Verification Request), который содержит информацию о торговце и номер карты плательщика. Этот запрос отправляется банку-эмитенту для проверки того, что 3DS для данной карты включен и ее можно использовать для оплаты. После получения ответа VeRes (Verification Response), в котором наиболее важным параметром является URL-адрес, который указывает, где находится сервер эквайера и куда необходимо отправить отправить PaReq. PaReq (Payment Request) – запрос на оплату, в котором передаются данные продавца, информация о платеже и URL-адрес платежного агрегатора, на который будет возвращен плательщик в конце процесса аутентификации 3D Secure. Запрос на оплату выполняется посредством перенаправления на сервер эквайера через браузер плательщика. На стороне эквайера плательщик вводит одноразовый код и возвращается на сайт платежного агрегатора вместе с результатом проверки PaRes (Payment Response). После получения успешного статуса верификации платежный агрегатор совершает запрос в банк эквайер на списание денежных средств.[3]

Несмотря на то, что данную версию протокола используют больше всего, она имеет ряд недостатков и проблем:

1. Протокол поддерживает только взаимодействие через браузерный интерфейс.
2. Верификация держателя карты осуществляется только с помощья смс-кодов.
3. Из-за использования формата XML данная версия уязвима к атакам типа XXE (XML external entity).
4. Потенциальная атака на магазин торговца из-за выполения PaReq в формате перенаправления.

II. Протокол 3D Secure 2.0

Из-за недостатков протокола 3D Secure 1.0 была создана усовершенствованная версия протокола - 3D Secure 2.0, который развивает EMVCo – организация, созданная международными платежными системами с целью разработки международных стандартов для чиповых карт и операций с ними.

В обновленном протоколе добавили гибкую поддержку различных устройств и каналов. Обеспечили более плавное и последовательное взаимодействие с плательщиком по нескольким каналам оплаты, включая оплату в браузере мобильного телефона, платежи в приложени-

ях и платежи через цифровой кошелек. Улучшили пользовательский опыт. Обеспечив продавцам возможность лучше интегрировать процесс аутентификации в процесс покупок, предоставляя держателям карт быструю, простую и удобную аутентификация при высоком уровне безопасности. В отличие от статических паролей, в 3D Secure 2.0 используются методы динамической аутентификации, такие как биометрия и аутентификация на основе токенов. Улучшили обмен данными для борьбы с мошенничеством и снижения препятствий. В протоколе 2.0 существует 2 варианта аутентификации:

1. Аутентификация с вводом одноразового пароля.
2. Беспрепятственная аутентификация.[1]

Беспрепятственная аутентификация позволяет эмитентам одобрить транзакцию, не требуя ручного ввода данных от владельца карты. Это достигается с помощью так называемой «аутентификации на основе рисков» (RBA). RBA работает, собирая набор данных о держателях карт во время транзакции и передавая их банку-эмитенту и его серверу, который затем сравнивает собранные данные с предыдущими (историческими) данными о транзакциях держателя карты для вывода значения риска мошенничества, соответствующего новой транзакции.

III. Алгоритм управления протоколом 3D Secure 2.0

В обновленной версии протокола 3D сервер платежного агрегатора взаимодействует напрямую в основном с корневым сервером платежной системы (Visa, MasterCard, Maestro). Перед началом работы алгоритма 3D сервер должен запросить у сервера платежной системы информацию о диапазонах номеров карт, которые поддерживают версию 2.0, с помощью подготовительного запроса (PReq). Кроме того 3D должен регулярно обновлять информацию о диапазонах. Данные сообщения не являются частью основного алгоритма.[2]

Алгоритм запускается в отдельном изолированном потоке и проверяет принадлежность карты плательщика к диапазонам, которые сохранены в 3D сервере платежного агрегатора. После подтверждения версии 3D сервер отправляет зашифрованный авторизационный запрос (AReq) на сервер платежной системы. В авторизационном запросе содержатся данные о торговце, покупке и информация о плательщике, например публичные данные его браузера. Именно на основании этих данных банк эмитент может разрешить беспрепятственную аутентификация. Если в ответе на авторизационный запрос банк подтвердил принадлежность карты плательщику, то алгоритм завершает верификацию и запускает следующий алгоритм в изолированном потоке, которые выполняет платежный запрос.

В случае, если банку эмитенту не хватило предоставленных данных, то алгоритм продолжает работу и выполняет дополнительный запрос верификации (CReq). Данный запрос, как и при использовании первой версии протокола, выполняется посредством перенаправления плательщика на страницу банка эмитента через его браузер. Как только плательщик пройдет дополнительную проверку корневой сервер платежной системы отправляет результаты на 3D сервере платежного агрегатора. После чего алгоритм завершает верификацию и запускает следующий алгоритм в изолированном потоке, которые выполняет платежный запрос.

Заключение

Рассмотренный метод управления безопасностью платежного агрегатор позволяет установить безопасный канал обмена данными, работающий в режиме реального времени, по которому будет передаваться намного больше данных о транзакции для более точной аутентификации покупателя, увеличится скорость совершения оплаты, поскольку аутентификацию с помощью пароля будут проходить не все транзакции, а только некоторая их часть. Описанный алгоритм управления протоколом 3D Secure 2.0 реализует все нововведения протоколоа, для обеспечения быстрых и надежный онлайн-платежей через банковские карты.

Список литературы

1. EMV3-D Secure Protocol and Core Functions Specification [Electronic resource] / EMVCo LLC. – United States, 2017. – Mode of access: https://www.emvco.com/emv-technologies/3d-secure/core-functions-specifications. – Date of access: 17.10.2021.
2. 3-D Secure Browser Flow Best Practices [Electronic resource] / EMVCo LLC. – United States, 2021. – Mode of access: https://www.emvco.com/emv-technologies/3d-secure/browser-flow-best-practices. – Date of access: 17.10.2021.
3. Requirement Numbering Scheme and Error Processing [Electronic resource] / EMVCo LLC. – United States, 2021. – Mode of access: https://www.emvco.com/emv-technologies/3d-secure/requirement-numbering-scheme-and-error-processing. – Date of access: 17.10.2021.