М. И. Оберемко

АЛГОРИТМЫ УПРАВЛЕНИЯ ПЛАТЕЖНЫМ АГРЕГАТОРОМ

Рассматриваются вопросы применения протокола 3-D Secure в качестве эффективного метода управления безопасностью платёжного агрегатора при проведении онлайн-операций с кредитными и дебетовыми картами.

Введение

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

В случае использования протокола 3-D Secure, кроме обеспечения дополнительного уровня защиты от мошенничества, происходит «перенос ответственности» за мошеннический платёж, т.е. вся ответственность переходит от продавца к банку-эмитенту, выпустившему карту. Данное преимущество протокола 3-D Secure позволяет бизнесу при использовании этого протокола повысить конверсию.

I. Алгоритм управления протоколом 3-D Secure 1.0

В настоящее время подавляющее большинство банков и платёжных систем используют версию 1.0 протокола 3-D Secure 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 платёжного агрегатора запускается следующий алгоритм. В первую очередь осуществляется CRReq-запрос (Card Range Request). Данный запрос необходим для нахождения банка-эмитента проверяемой карты и получения CRReq-запроса из домена взаимодействия. Далее агрегатор отправляет VeReq-запрос (Verification Request), содержащий информацию о торговце и номер карты плательщика. Этот запрос отправляется банку-эмитенту для проверки того, что протокол 3-D Secure для данной карты включён и её можно использовать для оплаты. После получения ответа VeRes (Verification Response), в котором наиболее важным параметром является URL-адрес, указывающий, где находится сервер эквайера и куда необходимо отправить PaReq-запрос. PaReq (Payment Request) — это запрос на оплату, в котором передаются данные продавца, информация о платеже и URL-адрес платёжного агрегатора, на который будет возвращен плательщик в конце процесса аутентификации 3-D Secure. Запрос на оплату выполняется посредством перенаправления на сервер эквайера через браузер плательщика. На стороне эквайера плательщик вводит одноразовый код и возвращается на сайт платёжного агрегатора вместе с результатом проверки PaRes. После получения успешного статуса верификации платёжный агрегатор совершает запрос в банк-эквайер на списание денежных средств [3].

Несмотря на то, что данную версию протокола используют чаще всего, она имеет ряд следующих недостатков:

- протокол поддерживает только взаимодействие через браузерный интерфейс;
- верификация держателя карты осуществляется только с помощью смс-кодов;
- из-за использования формата XML данная версия уязвима к атакам типа XXE (XML external entity);
- потенциальная атака на магазин торговца из-за выполнения PaReq-запроса в формате перенаправления.

II. Протокол 3-D Secure 2.0

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

В обновлённом 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 приложениях и платежи через цифровой кошелёк. Улучшили пользовательский опыт, обеспечили продавцам возможность глубже интегрировать проце-

дуру аутентификации в процесс покупок, предоставляя держателям карт быструю, простую и удобную аутентификация при высоком уровне безопасности. В отличие от статических паролей, в протоколе 3-D Secure 2.0 используются методы динамической аутентификации, такие как биометрия и аутентификация на основе токенов доступа. Улучшили обмен данными для борьбы с мошенничеством и снижения препятствий.

В протоколе версии 2.0 существуют два варианта аутентификации:

- аутентификация с вводом одноразового пароля;
- 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). Аутентификация 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 информацией о предыдущих транзакциях держателя карты для вывода значения риска мошенничества, соответствующего новой транзакции.

III. Алгоритм управления протоколом 3-D Secure 2.0

В обновленной версии протокола 3-D сервер платежного агрегатора взаимодействует напрямую в основном с корневым сервером платежной системы (Visa, MasterCard, Maestro). Перед началом работы алгоритма 3-D сервер должен запросить у сервера платёжной системы информацию о диапазонах номеров карт, которые поддерживают версию 2.0, с помощью подготовительного запроса (PReq). Кроме того, 3-D сервер 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 3-D сервере платёжного агрегатора. После успешной проверки 3-D сервер отправляет зашифрованный авторизационный запрос (AReq) на сервер платёжной 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 процедуру верификации и запускает следующий алгоритм в изолированном потоке, который выполняет платёжный запрос. В случае если банку-эмитенту не хватило предоставленных данных, то алгоритм продолжает работу и выполняет дополнительный запрос верификации (CReq). ДДанный 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 платёжной системы отправляет результаты на 3-D сервер платёжного агрегатора. После этого алгоритм завершает верификацию и запускает следующий алгоритм в изолированном потоке, который выполняет платёжный запрос.

Заключение

Рассмотренный алгоритм управления безопасностью платёжного агрегатора позволяет установить работающий в режиме реального времени безопасный канал обмена данными, 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 3-D Secure 2.0 реализует все нововведения протокола, для обеспечения быстрых и надёжных онлайн-платежей посредством банковских карт.

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.

Оберемко Максим Игоревич, магистрант кафедры информационных технологий автоматизированных систем БГУИР, oberemko.maxim@gmail.com.

Научный руководитель: Севернёв Александр Михайлович, доцент кафедры ИТАС БГУИР, кандидат технических наук, severnev@bsuir.by.