March 2023

Risk-based Payment Authorization for Online Transactions

Stan Li

Aneesh Ali Nainamvalappil Cheriyakath

Archana Malhotra

Risk-based Payment Authorization for Online Transactions

ABSTRACT

This disclosure describes techniques for risk-based authentication and/or authorization of payments for transactions. Per techniques of this disclosure, risk signals associated with a transaction initiated from a user device are determined based on user-permitted factors. The risk signals are transmitted to a payment instrument issuer prior to the initiation of a payment authorization request. The payment instrument issuer can determine the risk associated with a transaction based on the risk signals. If the determined risk exceeds a threshold, the payment instrument issuer may request additional user verification, e.g., via a challenge-response mechanism. Payment credentials are provided based on the determined risk.

KEYWORDS

- Online payment
- Online transaction
- Payment platform
- Payment wallet
- Payment application
- Transaction risk
- Payment processor
- Payment Fraud

BACKGROUND

Online transactions require users to make use of payment instruments such as credit or debit cards, payment wallets, payment apps, etc. When making a payment, payment credentials associated with a payment instrument, e.g., card number, expiry, card verification code (CVC),

etc. are transmitted from a user device to a payment processor such as a card issuer for authorization (approval) of the payment. Current transaction authorization workflows typically only enable the issuer to make an authorization decision in a binary fashion (approve or decline) based on the received static payment credentials. The authorization workflow commences after the payment authorization is requested by the user, e.g., after a user clicks a checkout button to initiate an online transaction. This can contribute to higher fraud (if fraudulent transactions are approved) or poor user experience (if legitimate transactions are declined).

DESCRIPTION

This disclosure describes techniques for risk-based authentication and/or authorization of payments for transactions. Per techniques of this disclosure, risk signals are determined and transmitted to a payment instrument issuer such a card issuer and/or payment wallet/app provider prior to obtaining payment credentials and the initiation of a payment authorization request. In some scenarios, based on the determined risk, additional user verification can be sought to mitigate the risk of fraud.

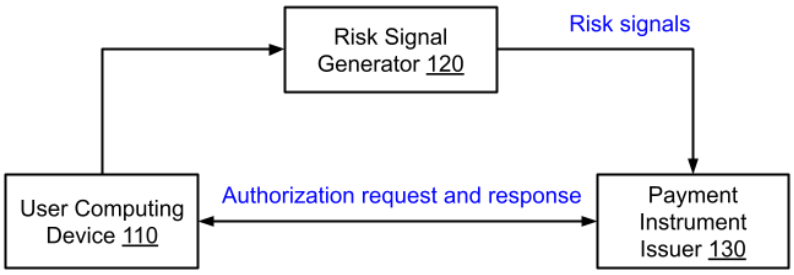

Fig. 1: System architecture for risk-based transaction payment authorization

Fig. 1 depicts an example architecture for risk-based transaction payment authorization, per techniques of this disclosure. As depicted in Fig. 1, with user permission and express consent, user information obtained from a user computing device (110) is utilized to generate

risk signals for payment transactions at a risk signal generator (120). In some implementations, the risk signals may be generated at the user computing device itself. The risk signals are provided to a payment instrument issuer (130) such as a card issuer computing system. Based on the risk signals, the payment instrument issuer may optionally request additional user verification.

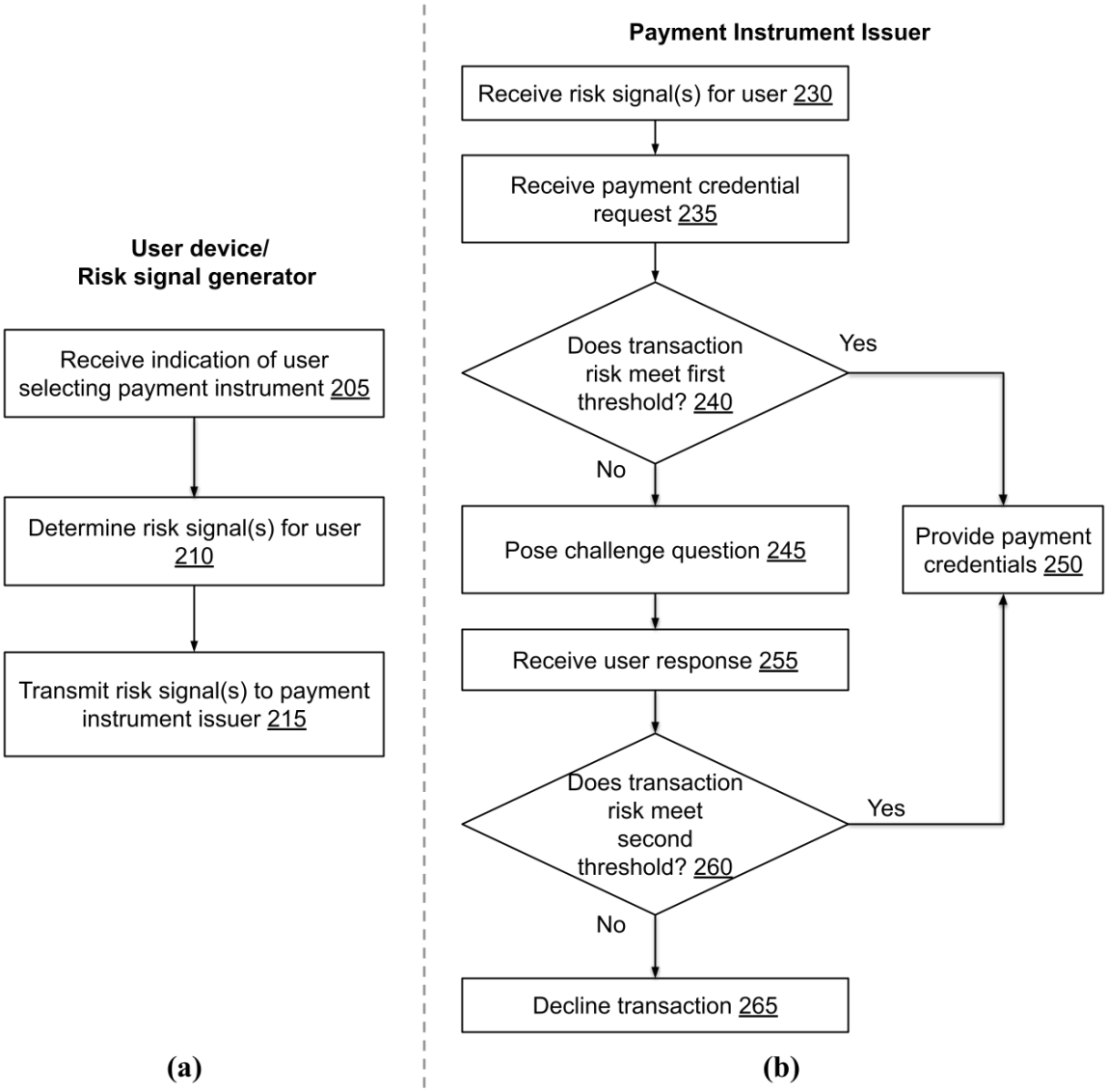

Fig. 2: Workflow for risk-based transaction payment authorization

Fig. 2 depicts an example workflow for risk-based payment transaction authorization, per techniques of this disclosure. Fig. 2(a) depicts the workflow at a user device and/or a risk signal generator. An indication of a user selecting a payment instrument is received (205). With user permission and express consent, risk signal(s) are determined (210) for the user, based on available user-permitted information. Such information may include the user's prior activity, user account data, device-specific factors, merchant-specific factors, etc. The risk signals(s) are transmitted (215) to a payment instrument issuer.

Fig. 2(b) depicts the workflow at a payment instrument issuer, per techniques of this disclosure. Risk signal(s) are received (230) at the payment instrument issuer, e.g., from a risk signal generator and/or user device. A payment credential request is received (235). Based on the risk signals, it is determined (240) whether the transaction meets a first risk threshold. If it is determined that the transaction meets a first risk threshold (e.g., is determined to be low risk), the payment credentials are provided (250).

If it is determined that the transaction does not meet the first risk threshold (e.g., is determined to not be of low risk), a suitable challenge question is determined and transmitted (245) to the user. A user response is received (255). Based on the received response, it is determined (260) whether the transaction meets a second risk threshold. In some implementations, the first risk threshold and the second risk threshold may be the same. If it is determined that the transaction meets the second risk threshold, the payment credentials are provided(250). If it is determined that the transaction does not meet the second risk threshold, the transaction is declined (265).

Techniques of this disclosure can be utilized to provide timely evaluation of transaction risk (e.g., by initiating risk signal generation when a user selects a payment instrument rather

than at checkout) in addition to providing layered control of authorization (selective use of challenge-response mechanism) beyond just approval and declining of a transaction. The techniques can be used in any application or platform, e.g., an operating system, a browser, a payment wallet or payment application, etc. Such applications can thus provide ease of use through use of autofill whereby stored payment credentials are automatically entered in a transaction user interface while ensuring risk of a fraudulent transaction is reduced.

Further to the descriptions above, a user may be provided with controls allowing the user to make an election as to both if and when systems, programs, or features described herein may enable the collection of user information (e.g., information about a user's social network, user account data, user device information, social actions or activities, profession, a user's preferences, or a user's current location), and if the user is sent content or communications from a server. In addition, certain data may be treated in one or more ways before it is stored or used so that personally identifiable information is removed. For example, a user's identity may be treated so that no personally identifiable information can be determined for the user, or a user's geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level) so that a particular location of a user cannot be determined. Thus, the user may have control over what information is collected about the user, how that information is used, and what information is provided to the user.

CONCLUSION

This disclosure describes techniques for risk-based authentication and/or authorization of payments for transactions. Per techniques of this disclosure, risk signals associated with a transaction initiated from a user device are determined based on user-permitted factors. The risk signals are transmitted to a payment instrument issuer prior to the initiation of a payment

authorization request. The payment instrument issuer can determine the risk associated with a transaction based on the risk signals. If the determined risk exceeds a threshold, the payment processor may request additional user verification, e.g., via a challenge-response mechanism. Payment credentials are provided or declined based on the determined risk.