October 06, 2017

Automatic execution of authentication actions at high trust levels

Thomas Price

Justin Lewis

Automatic execution of authentication actions at high trust levels

ABSTRACT

Online authentication systems for payment, electronic commerce, personal communication, etc. are increasingly subject to attacks. If breached, such systems can permit fraudulent transactions. As a result, software applications (apps), e.g., e-commerce apps, banking apps, etc. deploy additional levels of identity authentication to verify user identity for sensitive transactions, e.g., money transfer from a new device, ordering goods to a new delivery address, etc. This disclosure proposes queueing actions that require additional levels of authentication such that such actions are executed at a later time once a high level of trust is obtained. High level of trust can be obtained in various ways, e.g., when the user uses the app or service from a trusted device, when the user device is at a trusted location or connects to a trusted network, the user device is close to another device that the user is signed into, etc.

KEYWORDS

- Authentication
- Internet security
- Trusted environment
- Trusted device
- Online transaction
- Queued transaction

BACKGROUND

With increasingly higher number of apps, online vendors, and services, user authentication for tasks such as payments has acquired significant importance. Service providers, such as bank, e-commerce vendors, e-mail providers, etc. rely on being able to verify the identity of a customer to grant or deny access to information and assets. Fraudulent authentication, e.g., due to stolen passwords, phishing, pharming, and other attacks, can lead to a vendor providing access to unauthorized individuals and result in monetary fraud.

For example, e-commerce applications provide customers and merchants with a quick and convenient way to exchange goods and services. Such applications utilize various online authentication technologies that authenticate users and verify user identity to protect customers and merchants from security threats. Other online services, e.g., e-mail, messaging, social networks, etc. also require user authentication. Some online user actions are more sensitive to fraud than others and for such actions, additional levels of authentication are employed. For example, such services can include sending money in a payment app from a new device, ordering to a new delivery address in an e-commerce app, changing an e-mail password, etc.

Currently, additional form of authentication involves users being prompted to take actions to prove their identity, e.g., enter a PIN-style code sent to a known email address or as a text message to their known phone number; re-enter a password; confirm the action via a pop-up prompt in an app on a second device; etc. The need for switching to a separate device or application and carrying out a second step, makes these types of actions difficult for users to carry out on-the-go on their mobile device. Often users need to abandon an action like a money transfer, and remember to take it up again later when it is feasible to find a one-time authorization code, or to re-attempt the action from another device that is more trusted by the service, e.g., a desktop computer.

DESCRIPTION

To make additional levels of authentication for sensitive transactions seamless to users, this disclosure utilizes a system where transactions that require a second form of authentication do not require additional proactive actions by the user for verification of user identity. Fig. 1 illustrates an example of the techniques of this disclosure where transactions requiring additional authentication are queued for automatic execution at a later time once a higher level of trust has been obtained.

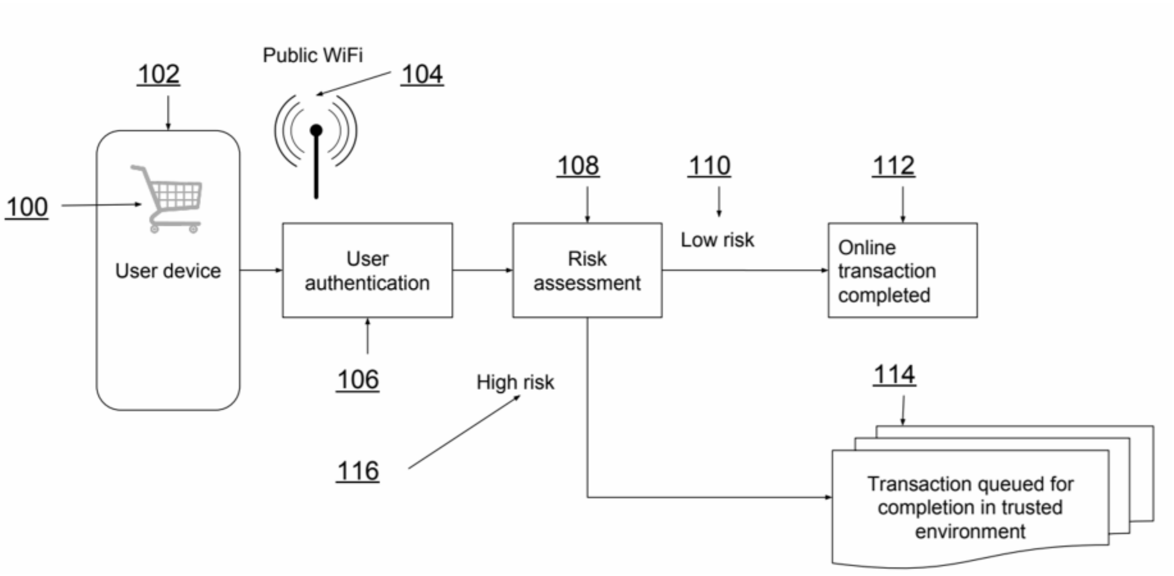

Fig.1: Transactions queued for completion in trusted environment

In the example illustrated in Fig. 1, a user uses an e-commerce app (100) on a user device (102), e.g., smartphone, tablet, etc. The user device is connected to a public Wi-Fi access point (104). When the user requests a transaction that is assessed as low risk (110) by risk assessment module (108), the transaction is completed without further authentication (112). For example, such transaction can include a purchase made with the user's authorized credit card and delivery address information saved in the e-commerce app.

When the risk assessment module determines the need for an additional level of user authentication, i.e., a high-risk transaction (116), the transaction is queued (114) for completion when a higher level of trust is established. Risk assessment can be performed on device, e.g., by the e-commerce app, or by a server that conducts the transaction.

When a transaction is queued for completion at a later time and when permitted by the user, a message is displayed on the user device. The message indicates to the user that the action is being queued for completion later, once a higher level of trust is obtained. At a later time, when the level of trust is higher, e.g., when the user is detected as active on a trusted device (e.g., home computer) or in a trusted environment (e.g., home network), the action (e.g., an e-commerce purchase transaction) is either executed automatically or the user is prompted to confirm execution of each previously-queued action, based on configurations as pre-set by the user.

Determination of a high level of trust is achieved passively, without user input, e.g., by detecting that the user device has connected to a trusted network; by detecting that the user device is within a short range of a second device such as a digital watch; by the user accessing the e-commerce app or service from a trusted device such as a home computer, etc. A user can set permissions for the factors that are used for the detection of trust level. Only such factors for which the user has provided permission are used to determine the trust level. If the user permissions do not enable automatically establishing the high trust level, the user is prompted to complete the transaction using traditional techniques such as authentication codes, reentry of password, etc.

The techniques described herein automatically determine the level of trust for a given user context, queue transactions when trust levels are low, and execute the queued transactions when a high trust level is established. This reduces the number of user actions and amount of user time required to perform actions that require an additional layer of security authentication beyond the user credentials that are already established at the time the user initially attempts the action. The techniques can positively impact metrics such as average abandonment and time-to-completion of e-commerce actions such as sending money or completing purchases.

Online services, e.g., e-commerce, e-mail, payment wallets, online software stores, etc., can use these techniques to lower the user effort required to complete the transaction, e.g., by eliminating the requirement of authorization codes or passwords. The techniques enable users to initiate transactions securely while on the go, e.g., using mobile devices such as smartphones, tablets, etc. The techniques are particularly suitable for providers of cross-platform services that are used on multiple devices and for hardware vendors that can rely on co-presence of devices to establish user identity.

Examples of use

Passive escalation of trust at a trusted location

A user attempts to order an item for delivery to a new address in a mobile e-commerce app. The app or the e-commerce vendor determines that the action needs further authentication. Without the techniques of this disclosure, the user is prompted to take further action to authenticate themselves. Such actions include, for example, re-entering a password, providing a one-time code transmitted by SMS or email, etc.

When the queueing techniques described herein are implemented, the transaction is queued, and the user is provided a message that indicates the queuing, e.g., due to pending verification of user identity. The message also indicates that the next time the user is in a more trusted environment, e.g., the user's home, the order will be carried out automatically. Once the user device is detected as being present at a trusted location, e.g., inside the user's home, a high level of trust is established. Detection of the trusted location can be based on the user device connecting to a trusted network (e.g., home network), or a smart home device. The order is carried out automatically with a notification on the user device that informs the user of the order completion. Alternatively, the notification can prompt the user to click to provide confirmation to carry out the action.

Money transfer from a new device

A user starts a transaction for a peer-to-peer money transfer using a money transfer app on a new tablet device. While the user is signed in on the tablet device, the user has not carried out prior payment transactions on the tablet device using the money transfer app. The money transfer app determines that higher level of trust in user identity is necessary to complete the money transfer.

The money transfer app pops up a notification on the user device that the payment can be sent out the next time the user is signed in on another device, e.g., a device from which the user used the money transfer app before. The notification includes the name of the device(s) that the payment is queued for later execution on, e.g., "next time you open the X-TPay app on your mobile phone." The user can choose to accept the queuing or to use a second authentication factor in the traditional manner, e.g., an authorization code emailed to the user's known email address, etc. If the user accepts the queueing of the money transfer request, the action is carried out automatically when a high level of trust is obtained. The money transfer is completed with a passive notification to the user, or the user is prompted for confirmation.

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 collection of user information (e.g., information about a user's social network, 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

The present disclosure queues transactions that require additional user authentication after an initial level of authentication is completed. Additional authentication is required when a risk associated with the transaction is high, e.g., a money transfer, an e-commerce order, a password change, etc. The queued transactions are executed at a later time when high levels of trust in the user identity is established. Online service providers can use these techniques to lower the user effort required to complete the transaction, e.g., by eliminating the requirement of authorization codes or passwords. The techniques enable users to initiate transactions securely while on the go, e.g., using mobile devices such as smartphones, tablets, etc. The techniques are particularly suitable for providers of cross-platform services that are used on multiple devices and for hardware vendors that can rely on co-presence of devices to establish user identity.