METHOD AND SYSTEM FOR INFORMATION AUTHENTICATION

Jinsai Chen

BACKGROUND

Field

[0001] The present application relates to the field of computer technologies, and in particular, to a method and system for information authentication.

Related Art

[0002] With the constant advancement of the computer and network technologies, it is common that users perform various operations via online accounts. For example, users may shop on e-commerce websites via accounts registered on these e-commerce websites.

[0003] However, along with the development of the computer and network technologies also comes an increasing amount of identity theft by unauthorized users. Once the account and password of a user are compromised, a malicious user may perform operations via the intercepted account, thereby causing great loss to the legitimate user.

[0004] Although a number of methods are available for increasing the difficulty in identity theft, the risk of such identity theft still remains.

SUMMARY

[0004a] The invention is defined in the independent claims. Optional features of the invention are defined in the dependent claims.

[0005] A system for facilitating multi-party authentication is provided. During operation, the system receives, via a communication module, an operation request from a primary user. The system then sends an authentication request to the authentication assistance user and receives a response from the authentication assistance user. Subsequently, the system allows or denies the operation request based on the response received from the authentication assistance user.

[0006] In a variation of this embodiment, prior to sending the authentication request, the system determines whether authentication from at least one authentication assistance user is required to allow the operation request.

[0007] In a variation of this embodiment, while determining whether authentication from at least one authentication assistance user is required, the system applies at least one predetermined rule to the received operation request.

[0008] In a further variation, the rule is based on a transaction type associated with the operation request.

[0009] In a further variation, the rule is based on a payment amount.

[0010] In a variation of this embodiment, the system further determines whether the response received from the at least one authentication assistance user indicates an approval metric that is greater than a predetermined threshold.

[0011] In a variation of this embodiment, while sending the authentication request to the authentication assistance user, the system sends the authentication assistance user a text message based on a phone number, an email, or an instant message.

[0012] In a variation of this embodiment, while denying the operation request, the system sends a reason for denial to the primary user.

BRIEF DESCRIPTION OF THE FIGURES

[0013] The accompanying drawings herein, which are incorporated herein and constitute a part of the specification, illustrate several exemplary embodiments of the present application and together with the description, serve to illustrate the present application, construing no limitation to the present application. In the drawings:

[0014] FIG. 1A illustrates an exemplary computing system that facilitates a multi-party authentication process, in accordance with an embodiment of the present application.

[0015] FIG. 1B illustrates a process of information authentication, in accordance with an embodiment of the present application.

[0016] FIG. 2 illustrates a detailed process of information authentication according to an embodiment of the present application; and

[0017] FIG. 3 illustrates an exemplary authentication system that facilitates multi-party authentication.

DETAILED DESCRIPTION

[0018] The techniques disclosed herein may solve the problem of improving the security of online transaction by allowing multiple parties, instead of a single party, to participate in an authentication process for the online transaction. Conventionally, an online transaction is allowed to proceed as long as a user enters a correct password or other types of user credentials of the corresponding online account. If the account name and password of the user are stolen, significant loss can occur. In addition, it is often the case that a single user is not the sole party in making the decision about an online transaction. For example, a minor might need both parents'

approval before making a large online purchase. In a corporate environment, a decision or online transaction might require multiple parties' approval to consummate.

[0019] One or more authentication assistance users may be allowed to be associated with the authentication process for an account. For instance, in addition to a primary user entering the correct password for the account, confirmation from a number of authentication assistance users can also be required to perform an online transaction associated with the account. In this way, even if the primary user's account information and password are stolen, losses may be effectively prevented because the online transaction may not be allowed to proceed without confirmation from other authentication assistance users.

[0020] To make the objectives, technical solutions, and advantages of the present application clearer, the technical solutions of the present application are hereinafter described in detail thoroughly with reference to the specific embodiments of the present application and the corresponding drawings. Clearly, the embodiments described herein are merely exemplary ones, but are not all the embodiments of the present application. Based on the embodiments of the present application, all other embodiments derived by persons of ordinary skill in the art without any creative efforts shall fall within the protection scope of the present application.

[0021] FIG. 1A illustrates an exemplary computing system that facilitates a multi-party authentication process, in accordance with an embodiment of the present application. In this example, an authentication server 110 is in communication with a primary user 101. Also coupled to authentication server 110 are authentication assistance users 102, 104, 106, and 108. A transaction server 112 (for example, an electronic-commerce merchant's datacenter) can be in communication with authentication server 110.

[0022] During operation, primary user 101 initiates a transaction request and sends the request to authentication server 110. Upon receiving this request, authentication server 110 sends an authentication request to assistance users 102, 104, 106, and 108. Each of these four assistance users can either approve or confirm the authentication request (for example, by providing their own authentication credentials such as a username and password), or deny the authentication request.

[0023] Once authentication server 110 receives approval or denial from the four assistance users 102, 104, 106, and 108, authentication server 110 can either allow the transaction requested by primary user 101 to proceed, or deny the transaction request from primary user 101. In one embodiment, when the transaction is approved to proceed, authentication server 110 can forward the transaction request to transaction server 112, which in turn processes the transaction request and consummates the corresponding transaction.

message returned by user *u*. If a short message with content "Y" is received from user *u*, the authentication server determines that authentication acknowledgement information returned by user *u* is received, and thus allows performing the operation corresponding to the payment request sent by the primary user (that is, allows the primary user to pay *x* to purchase merchandise *s* via account *A*); and if a short message with content "N" is received from the user *u*, the authentication server determines that user *u* has denied the authentication request, and thus denies performing the operation corresponding to the payment request sent by the primary user.

[0039] According to the above method, although the server may choose not to determine whether the primary user is the owner of the account, and the operation request may be allowed only when the authentication assistance user of the account acknowledges the operation request. Therefore, when the account and password of a user are intercepted, that is, when the primary user sending the operation request is not the owner of the account, even if an unauthorized user enters the correct password, the unauthorized user still cannot perform any operation via the account without the approval of the authentication assistance users. In this way, even if the account and password of the user are stolen, it may still be ensured that the owner of the account is not subjected to any loss.

[0040] In addition, the techniques disclosed may provide protection for underage users of the Internet. For example, a child's guardians can be set as the authentication assistance users of the accounts, and the operations to be performed by the child over the Internet may be allowed to perform only when the guardians acknowledge and allow the operations.

[0041] In general, the authentication server can implement rules to determine whether a received operation request would require additional approval from authentication assistance user(s). For example, in operation S101 as illustrated in FIG. 1B, when the operation request sent by the primary user via the account is a payment request, before the authentication server searches for the predetermined authentication assistance user corresponding to the account in operation S102, the server may determine whether the payment amount requested by the operation request is greater than a predetermined threshold. If the amount is greater than the threshold, the server determines that additional approval from authentication assistance user(s) is needed, and searches for the authentication assistance user corresponding to the account. Otherwise, the server may directly allow performing the operation corresponding to the operation request without requiring additional approval from the assistance user(s). The predetermined amount may be otherwise defined according to actual needs, or may be defined by the owner of the account, for example, $500.

[0042] Similarly, before the server searches for the predetermined authentication assistance user corresponding to the account, the server may also determine that the type of the

[0046] In a further example, if the system adopts a majority principle, i.e., as long as there are more assistance users giving approval than assistance users denying the request, then a ratio of 50% can be used. That is, as long as the ratio of approving assistance users to the total assistance users is greater than 50%, the authentication server can allow the operation request. Other ways of setting the threshold for allowing the operation request are also possible.

[0047] In a further embodiment, the authentication system can allow an assistance user to provide a reason for denying the authentication request. For example, the deny reason returned by an assistance user can be that "the account has been compromised, and the operation is not performed by the authorized user." The authentication server may further present the denial reason to the primary user upon denying the operation request.

[0048] FIG. 2 illustrates a detailed process of information authentication, according to an embodiment of the present application. During operation, the authentication server receives an operation request sent by a primary user via an account (operation S201). The authentication server then authenticates a password provided by the primary user (operation S202). If the password-based authentication fails, the authentication server denies the operation corresponding to the operation request (operation S208).

[0049] If the primary user's password based authentication is successful, the authentication server proceeds to search for predetermined authentication assistance user corresponding to the account through which the primary user has sent the operation request (operation S203). The authentication server then sends authentication inquiry information associated with the operation to the identified authentication assistance user(s) (operation S204).

[0050] Next, the authentication server computes the ratio of the authentication assistance users returning acknowledgement (i.e., approval) to the authentication assistance users denying authentication (operation S205). Note that in this example, the threshold is based on such a ratio as described above. Other formula, such as a percentage of the authentication users giving approval, or an absolute number of approving assistance users, can also be used.

[0051] The authentication server then determines whether the ratio is greater than a predetermined threshold (operation S206). If so, the authentication server allows performing the operation corresponding to the operation request (operation S207). Otherwise, the authentication server denies the operation (operation S208).

[0052] After performing an operation corresponding to the operation request is denied, denial reason information in the authentication denial information may be presented to the primary user.

[0053] FIG. 3 illustrates an exemplary authentication system that facilitates multi-party authentication. An authentication

What Is Claimed Is:

1. A computer-implemented method for facilitating multi-party authentication, the method comprising:

receiving, from a primary user, an operation request requiring approval from authentication assistance users specified by the primary user;

sending an authentication request to the authentication assistance users;

receiving a response from the authentication assistance users;

computing a ratio of a number of authentication assistance users indicating an approval response to a number of total authentication assistance users; and

allowing or denying the operation request based on whether the ratio is greater than a predetermined threshold.

2. The method of claim 1, further comprising:

determining a type of operation in the operation request; and

in response to determining that the type is not a first predetermined type of operation which requires approval from the authentication assistance users, allowing the operation request.

3. The method of claim 2, wherein determining whether the type is the first predetermined type comprises applying at least one predetermined rule to the received operation request.

4. The method of claim 3, wherein the rule is based on a transaction type associated with the operation request.

5. The method of claim 3, wherein the rule is based on a payment amount.

6. The method of claim 1, further comprising determining whether the response received from the authentication assistance users indicates an approval metric that is greater than a predetermined threshold.

7. The method of claim 1, wherein sending the authentication request to the authentication assistance users comprises sending the authentication assistance users a text message based on a phone number, an email, or an instant message.

8. The method of claim 1, wherein denying the operation request comprises sending a reason for denial to the primary user.

9. A non-transitory storage medium storing instructions, which when executed by a processor cause the processor to perform a method for facilitating multi-party authentication, the method comprising:

receiving, from a primary user, an operation request requiring approval from authentication assistance users specified by the primary user;

sending an authentication request to the authentication assistance users;

receiving a response from the authentication assistance users;

computing a ratio of a number of authentication assistance users indicating an approval response to a number of total authentication assistance users; and

allowing or denying the operation request based on whether the ratio is greater than a predetermined threshold.

10. The non-transitory storage medium of claim 9, wherein the method further comprises:

determining a type of operation in the operation request; and

in response to determining that the type is not a first predetermined type of operation which requires approval from the authentication assistance users, allowing the operation request.

11. The non-transitory storage medium of claim 10, wherein determining whether the type is the first predetermined type comprises applying at least one predetermined rule to the received operation request.

12. The non-transitory storage medium of claim 9, wherein the method further comprises determining whether the response received from the authentication assistance users indicates an approval metric that is greater than a predetermined threshold.

13. The non-transitory storage medium of claim 9, wherein sending the authentication request to the authentication assistance users comprises sending the authentication assistance users a text message based on a phone number, an email, or an instant message.

14. The non-transitory storage medium of claim 9, wherein denying the operation request comprises sending a reason for denial to the primary user.

15. A computer system for facilitating multi-party authentication, the computer system comprising:

a processor;

a memory coupled to the processor and storing instructions, which when executed by the processor cause the processor to perform a method, the method comprising:

receiving, from a primary user, an operation request requiring approval from authentication assistance users specified by the primary user;

sending an authentication request to the authentication assistance users;

receiving a response from the authentication assistance users;

computing a ratio of a number of authentication assistance users indicating an approval response to a number of total authentication assistance users; and

allowing or denying the operation request based on whether the ratio is greater than a predetermined threshold.

16. The computer system of claim 15, wherein the method further comprises:

determining a type of operation in the operation request; and

in response to determining that the type is not a first predetermined type of operation which requires approval from the authentication assistance users, allowing the operation request.

17. The computer system of claim 16, wherein determining whether the type is the first predetermined type comprises applying at least one predetermined rule to the received operation request.

18. The computer system of claim 15, wherein the method further comprises determining whether the response received from the authentication assistance users indicates an approval metric that is greater than a predetermined threshold.

19. The computer system of claim 15, wherein denying the operation request comprises sending a reason for denial to the primary user.

20. The method of claim 1, further comprising:

receiving a threshold-defining request from the primary user to specify predetermined threshold of authentication assistance users required to approve a type of operation requested by the primary user.