

METHOD AND SYSTEM FOR INFORMATION AUTHENTICATION

Jinsai Chen

5

BACKGROUND

Field

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

10

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.

15

[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.

20

[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.

25

[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.

30

[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.

5 [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.

10 [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

15 [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.

20 [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

25 [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.

[0024] Note that assistance users 102, 104, 106, and 108 can be pre-determined by primary user 101 and be associated with primary user 101's account. Optionally, these assistance users can also be specified by an entity other than primary user 101. For example, in a corporate environment, primary user 101 can be an employee responsible for purchasing office equipment. For certain type of purchases, assistance users 102, 104, 106, and 108 can be managers from different departments, and approval from all these four assistance users is needed for a purchase order to go through.

[0025] It is also possible for authentication server 110 to implement a set of rules, such that certain transactions requested by primary user 101 can be approved by authentication server 110 without additional approval from any assistance user, while transactions that satisfy the rules would require additional approval from assistance users to proceed. For example, primary user 101 could be a college student, who uses a credit card provided by his parents to pay for living expenses. Authentication server 110 can be part of the credit card company's services. Authentication server 110 can store a set of rules that require certain types of transactions requested by primary user 101 to be approved by additional assistance users. For instance, a rule might specify that certain type of transactions under a given amount, such as payment for food or gas that is less than \$100, can be processed without additional approval. Other types of payment, for example, a payment for electronic equipment, a payment for entertainment, or a payment that exceeds a predetermined limit, will require additional approval from the student's parents to be processed.

[0026] Note that the communication between authentication server 110 and a respective assistance user can be of any form. For example, authentication server 110 can send an email, a text message, or initiate a voice call to assistance user 102 to obtain the approval.

[0027] FIG. 1B illustrates a process of information authentication in accordance with an embodiment of the present application. During operation, the authentication server receives an operation request that is sent by a primary user via an account that belongs to the primary user (operation S101). Note that when the primary user desires to perform an operation or transaction via the account, the primary user firstly needs to send an operation request to the authentication server. The operation request can include, but is not limited to, a payment request. Furthermore, the primary user is not necessarily the owner of the account. Since the operation request only carries account information, the authentication server may optionally choose not to determine whether the primary user is the owner of the account.

[0028] For example, when the primary user shops on an e-commerce website, the primary user may purchase a piece of merchandise via an account A registered on the e-commerce website, and the primary user may send a payment request to an authentication server of the e-

commerce website via the account *A* (the payment request is the operation request), wherein since the payment request only carries information of the account *A*, in this case, the authentication server may choose not to determine whether the primary user is the owner of the account *A*.

5 **[0029]** Subsequently, the authentication server searches for a predetermined authentication assistance user corresponding to the account (operation S102). The authentication assistance user corresponding to the account may be predetermined by the owner of the account. Upon receiving the operation request sent by the primary user via the account, the authentication server may authenticate the password of the account entered by the primary user. If the password
10 based authentication is successful, the authentication server may search for the authentication assistance user that is predetermined for the account by the owner of the account and contact information of the authentication assistance user. If the password based authentication fails, the server may directly deny performing the operation corresponding to the operation request without contacting any authentication assistance user.

15 **[0030]** The contact information of the authentication assistance user can include, but is not limited to: a mobile phone number, instant messaging account information, email address, an account on the same authentication server, or any form of user identifier in a secure messaging system of the authentication assistance user.

[0031] Still using the above example, with respect to the account *A*, the owner of the
20 account *A* may predetermine a user *u* as a corresponding authentication assistance user, and store the contact information of user *u* on the authentication server. When receiving the payment request that is sent by the primary user via the account *A*, the authentication server first authenticates the password of account *A*; if the authentication is successful, the server may search for the contact information of authentication assistance user *u* corresponding to account *A*; and if
25 the authentication fails, the server may directly deny the operation request.

[0032] Next, the authentication server sends authentication inquiry information with respect to the operation request to the identified authentication assistance user (operation S103). Upon identifying the authentication assistance user corresponding to the account and the contact information of the authenticated assistance user, the authentication server may send the
30 authentication inquiry information with respect to the operation request to the authentication assistance user.

[0033] For example, when the contact information of the identified authentication assistance user is a mobile phone number, the authentication server may send the authentication inquiry information with respect to the operation request to the identified authentication
35 assistance user via a text message. When the contact information of the authentication assistance

user is an instant messaging account, the authentication server may send the authentication inquiry information with respect to the operation request to the assistance user's instant messaging account.

[0034] Furthermore, using the same example described above, the server may send
5 information of the merchandise ordered by the primary user indicated in the payment request, the payment amount requested, time information of the payment request, and the like to assistance user u via a text or instant message, to inquire whether assistance user u acknowledges the payment by the primary user. For example, the authentication server may send a short message
10 “Account A is purchasing merchandise s at time hh:mm, and is now requesting payment of x ; reply with Y to confirm, or reply with N to deny” to the mobile phone number of user u .

[0035] If the contact information of the authentication assistance user is an instant messaging account or an email address, the above authentication inquiry information may also be sent to the corresponding instant messaging account or email address. If the contact information of the assistance user is an account on the authentication server, upon determining that the
15 authentication assistance user has logged into the system via the account, the authentication server may also push the authentication inquiry information to the authentication assistance user via a message, a link to a webpage, or an alert.

[0036] The authentication server then determines whether authentication acknowledgement information returned by the authentication assistance user is received
20 (operation S105). If the authentication acknowledgement information is not received, or if the assistance user returns a disapproval or denial, the authentication server denies the operation request (operation S106). If no information is received from the authentication assistance user within a predetermined time duration (for example, 5 minutes), the server may consider that the authentication assistance user has denied the operation request.

[0037] If the authentication server receives authentication acknowledgement information returned by the authentication assistance user, the authentication server can allow performing the operation corresponding to the operation request (operation S105). If no information is received from the authentication assistance user within a predetermined time duration (for example, 5
25 minutes), the server may consider that the authentication assistance user denies the operation request, that is, the server considers that the authentication assistance user has returned authentication deny information and thus furthers relevant processing.

[0038] Still using the above example, upon sending the short message “Account A is purchasing merchandise s at time hh:mm, and is now requesting payment of x ; reply with Y to confirm, or reply with N to deny” to the mobile phone number of the authentication assistance
35 user u associated with account A , the authentication server may monitor the content of the short

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

received operation request is a predetermined operation request type. If the type of the received operation request is a predetermined operation request type, the server searches for the predetermined authentication assistance user corresponding to the account, to inquire whether the authentication assistance user acknowledges the operation request. Otherwise, the server may directly allow performing the operation corresponding to the operation request. The predetermined type of operation request may be a payment request, a user information change request, or the like. For instance, the authentication server may require additional approval from authentication assistance users only when the operation request sent by the primary user is a payment request or a user information change request. With respect to other types of operation requests (for example, a login request, a commodity inquiry request, or the like), the operation may be directly allowed.

[0043] As such, if the authentication server determines, based on predetermined rules or thresholds, not to require additional approval from authentication assistance user(s), the authentication server may allow performing the operation corresponding to the operation request after the primary user enters the correct password. Furthermore, the server may send a predetermined security question corresponding to the account to the primary user, and may allow performing the operation only after the primary user correctly answers the security question.

[0044] In some embodiments, the owner of the account may predefine a plurality of authentication assistance users for the account, and only a subset of approvals from all the authentication assistance users is needed to approve the operation request. For example, the authentication server may identify the authentication assistance users corresponding to the account, and send authentication inquiry information to these assistance users. The authentication server can then determine whether a ratio of the number of authentication assistance users returning authentication acknowledgement information to the number of total authentication assistance users is greater than a predetermined threshold. If the ratio is greater than the threshold, the server allows the operation request. Otherwise, the server denies the operation request. The predetermined threshold may be defined according to actual needs, or may be defined by the owner of the account.

[0045] For example, with respect to the account A, assume that the owner of the account A predefines n authentication assistance users, then according to the criterion that the operation is not allowed to perform as long as one authentication assistance user denies performing the operation, the predetermined threshold (which is the absolute number of assistance users giving approval) may be defined to be $n-1$. As such, the authentication server only allows the operation request when all the authentication assistance users returns approval for the request.

[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.

5 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
10 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
15 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
20 (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
25 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
30 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
35 authentication. An authentication

system 300 includes a processor 310, a memory 320, and a storage device 330. Storage 330 typically stores instructions that can be loaded into memory 320 and executed by processor 310 to perform the methods described above. In one embodiment, the instructions in storage 330 can implement a communication management module 332, an assistance user management module 334, an authentication module 336, and an operation request management module 338, all of which can communicate with each other through various means.

[0054] In some embodiments, modules 332, 334, 336, and 338 can be partially or entirely implemented in hardware and can be part of processor 310. Further, in some embodiments, the system may not include a separate processor and memory. Instead, in addition to performing their specific tasks, modules 332, 334, 336, and 338, either separately or in concert, may be part of special-purpose computation engines.

[0055] Storage 330 stores programs to be executed by processor 310. Specifically, storage 330 stores a program that implements a system (application) for enabling multi-party authentication. During operation, the application program can be loaded from storage 330 into memory 320 and executed by processor 310. As a result, system 300 can perform the functions described above. System 300 can be further coupled to an optional display 380, a keyboard 360, and a pointing device 370, and can be coupled via one or more network interfaces to a network 382.

[0056] During operation, communication management module 332 receives an operation request from a primary user via, for example, a communication port on system 300 (such as a network interface card). Upon authenticating the primary user with his individual credentials, assistance user management module 334 identifies one or more assistance users associated with the account via which the primary user sends the operation request. Subsequently, authentication module 336 sends authentication inquiries to the identified assistance users, and receives the corresponding responses. Based on the responses received from the assistance users, authentication module 336 determines whether a sufficient number of authentication acknowledgements (approvals) have been received. Accordingly, operation request management module 338 determines whether to allow or deny the operation request.

[0057] In some embodiments, assistance user management module 334 can determine whether assistance user approval is necessary based on certain rules applied to the operation request (such as a payment amount threshold or the type of online transaction corresponding to the operation request). In addition, authentication module 336 can apply a predetermined threshold for received approvals from the assistance users.

[0058] The data structures and computer instructions described in this detailed description are typically stored on a computer-readable storage medium, which may be any

device or medium that can store code and/or data for use by a computer system. The computer-readable storage medium includes, but is not limited to, volatile memory, non-volatile memory, magnetic and optical storage devices such as disk drives, magnetic tape, CDs (compact discs), DVDs (digital versatile discs or digital video discs), or other media capable of storing computer-readable media now known or later developed.

[0059] The methods and processes described in the detailed description section can be embodied as code and/or data, which can be stored in a computer-readable storage medium as described above. When a computer system reads and executes the code and/or data stored on the computer-readable storage medium, the computer system performs the methods and processes embodied as data structures and code and stored within the computer-readable storage medium.

[0060] Furthermore, methods and processes described herein can be included in hardware modules or apparatus. These modules or apparatus may include, but are not limited to, an application-specific integrated circuit (ASIC) chip, a field-programmable gate array (FPGA), a dedicated or shared processor that executes a particular software module or a piece of code at a particular time, and/or other programmable-logic devices now known or later developed. When the hardware modules or apparatus are activated, they perform the methods and processes included within them.

[0061] The above description is presented to enable any person skilled in the art to make and use the embodiments, and is provided in the context of a particular application and its requirements. Various modifications to the disclosed embodiments will be readily apparent to those skilled in the art, and the general principles defined herein may be applied to other embodiments and applications without departing from the spirit and scope of the present disclosure. Thus, the present invention is not limited to the embodiments shown, but is to be accorded the widest scope consistent with the principles and features disclosed herein.

What Is Claimed Is:

1. A computer-implemented method for facilitating multi-party authentication, the method comprising:
 - 5 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;
 - 10 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:
 - 15 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.
- 20 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
25 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
30 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.

5 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,
10 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;

15 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.

20 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
25 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.

30 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.

5 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;

10 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;

15 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.

20 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
25 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.

5 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
10 threshold of authentication assistance users required to approve a type of operation requested
by the primary user.