February 02, 2015

USER ACCOUNT AUTHENTICATION DURING USER ISSUE RESOLUTION

Alejo Grigera

Follow this and additional works at: http://www.tdcommons.org/dpubs_series

Recommended Citation
Grigera, Alejo, "USER ACCOUNT AUTHENTICATION DURING USER ISSUE RESOLUTION", Technical Disclosure Commons, (February 02, 2015)
http://www.tdcommons.org/dpubs_series/18
ABSTRACT

An authentication system generates a one time password (OTP) that is delivered to a user to authenticate a service representative’s request to access the user’s account. The system receives a request from the service representative to access the user’s account. The system generates the OTP and a summary of user’s account details requested for access by the service representative. Further, the system transmits the OTP and summary to the user. The system further authenticates the customer service’s request to access the user’s account based on the OTP and provides access of the requested account details to the service representative.

PROBLEM STATEMENT

Users contact customer service for assistance resolving problems related to services, e.g., cable, credit card, cellular phones, or Internet, they are using. A service representative is appointed to provide technical support to the customer. The service representative can access the customer’s account in order to diagnose the service problem and fix it. Generally, the service representative has complete access of the user’s account information. However, the service representative may require only limited access to the customer’s account information to resolve the problem. This can unnecessarily cause privacy concerns for the customer if the service representative accesses the customer’s private data that is not relevant to the customer’s service problem. For example, the service representative could view the customer’s account details, e.g., interests, usage, channels or T.V. shows watched, credit card transactions made, or web sites surfed. The service representative could further invade the customer’s privacy by showing or
discussing the customer’s account details to others. A method and system that allows a user to authenticate a service representative’s level of access to a user’s account, is described.

**AUTHENTICATION SYSTEM**

The system and techniques described in this disclosure relate to an authentication system that allows a user to authenticate a service representative’s request to access a user’s account. The authentication system can be implemented for use in an Internet, an intranet, or another client and server environment. The authentication system can be program instructions implemented locally on a client device or implemented across a client device and server environment. The client device can be any electronic device such as a mobile device, a smartphone, a tablet, a handheld electronic device, a wearable device etc.

Fig. 1 illustrates an example method 100 for authenticating a service representative’s request to access a user’s account. Method 100 can be performed by a system that authenticates a service representative’s level of access to the user’s account to resolve the user’s service problem, e.g., the authentication system.

A user may be in a conversation with a service representative to resolve a problem that the user is facing. The conversation may take place over telephone, instant messaging, e-mails video chat, etc. In order to analyze the user’s problem, the service representative may require access to certain details of the user’s account. Therefore, the service representative requests access to the user’s account. The authentication system or any service account portal that uses the authentication system can facilitate the service representative’s access to the user’s account. For example, the service representative can submit a request for access to the system. The
request for access can identify the user account to be accessed, e.g., with an account identifier or name of the user. The request can further identify a level of access requested by the service representative. For example, the service representative can detail whether he needs only limited or complete access to the user’s account. As a further example, the service representative can identify specific details of the user account that he needs to access to service the user’s account.

The system receives the request from the service representative to access the user’s account (block 110).

In response to the request, the system generates a one time password (OTP) and a summary of the account details requested by the service representative for access (block 120). The OTP is a password that is valid for only one login session or transaction with the user’s account. The OTP can be a random code consisting of alphabets and/or numerical digits. The system may include a server or a processor to execute an OTP generating algorithm that uses randomness or hash functions to generate the OTP. The OTP may be valid for a limited amount of time. For example, the OTP expires ten minutes after it is generated and can no longer be used to access the user’s account. The system generates the summary of the account details requested by the service representative by identifying the user’s account details that the service representative will be able to access if his request is granted. The summary indicates the level of access requested by the service representative. The level of access may be identified in the form of text, a corresponding image, video, screenshot, etc. The summary can also describe the user’s specific account details that can be viewed by the service representative if the service representative is granted the requested level of access. For example, the summary describes the
history of T.V. programs that the user watched which will be accessible to the service representative.

The system further transmits the generated OTP and the summary of requested account details to the user (block 130). The system may transmit the OTP and the summary to an electronic device associated with the user. The system may transmit the OTP and summary through a text message, e-mail, telephonic call, etc. The summary of the requested account details helps in informing the user about the information that can be accessed by the service representative, i.e., level of access to user’s account, as requested by the service representative. This allows the user to decide whether the requested level of access is appropriate.

On receiving the OTP and the summary, the user may decide to provide access of the requested account details to the service representative. The user can then communicate the received OTP to the service representative. The service representative then submits the OTP received from the user to the system for authentication. The system validates the OTP received from the service representative. For example, the system matches the OTP received from the service representative with the original OTP generated and transmitted to the user. Hence, the system authenticates the service representative’s request to access the user’s account based on the OTP (block 140).

Based on the authentication, the system provides access of the requested account details to the service representative (block 150). The service representative may then analyze the user’s account details in order to resolve the problem. Once the problem is resolved and the user terminates the conversation, the system may terminate service representative’s access to the
user’s account. The method 100 makes levels of requested access clear to the user and allows the user to make informed decisions in granting access to his account.

Fig. 2 shows an example workflow 200 of the authentication system. As shown in Fig. 2, a user is in a conversation with a customer service representative (CSR) in order to resolve a problem (step 205). The user may communicate with the CSR via telephone, instant messaging, e-mails, video chat, etc. In order to analyze user’s problem, the CSR requests access to certain details of the user’s account from the system (step 210). The CSR request for a particular level of access to the user’s account may vary from complete access to a limited access of specific details that are required to fix the problem.

On receiving the request, the system generates a one time password (OTP) and a summary of the account details requested for access. The system further transmits the generated OTP and the summary to the user, e.g., via a text message or e-mail. (step 220). The user receives the OTP and summary and can review the level of access requested by the CSR. At this point, the user can decide whether the requested level of access is appropriate for resolving the problem. If the user considers the level of access appropriate, then the user may provide the CSR with the received OTP (step 225), which is then submitted by the CSR to the system for verification (230).

If the received OTP matches the transmitted OTP, the system provides access of the requested account details to the CSR (step 235). The CSR analyzes the user’s account details to troubleshoot the problem (step 240). Once the CSR has resolved the problem, the user may terminate the conversation with the CSR (step 245). On termination of the conversation, the system terminates CSR’s access to the user’s account (step 250). The example scenario 200
ensures that the CSR does not have access to unnecessary information related to user’s account, and hence provides better customer service experience and helps in reducing risk of privacy breaches.

Fig. 3 is a block diagram of an exemplary environment that shows components of a system for implementing the techniques described in this disclosure. The environment includes client devices 310, servers 330, and network 340. Network 340 connects client devices 310 to servers 330. Client device 310 is an electronic device. Client device 310 may be capable of requesting and receiving data/communications over network 340. Example client devices 310 are personal computers (e.g., laptops), mobile communication devices, (e.g. smartphones, tablet computing devices), set-top boxes, game-consoles, embedded systems, and other devices 310’ that can send and receive data/communications over network 340. Client device 310 may execute an application, such as a web browser 312 or 314 or a native application 316. Web applications 313 and 315 may be displayed via a web browser 312 or 314. Server 330 may be a web server capable of sending, receiving and storing web pages 332. Web page(s) 332 may be stored on or accessible via server 330. Web page(s) 332 may be associated with web application 313 or 315 and accessed using a web browser, e.g., 312. When accessed, webpage(s) 332 may be transmitted and displayed on a client device, e.g., 310 or 310’. Resources 318 and 318’ are resources available to the client device 310 and/or applications thereon, or server(s) 330 and/or web pages(s) accessible therefrom, respectively. Resources 318’ may be, for example, memory or storage resources; a text, image, video, audio, JavaScript, CSS, or other file or object; or other relevant resources. Network 340 may be any network or combination of networks that can carry data communication.
The subject matter described in this disclosure can be implemented in software and/or hardware (for example, computers, circuits, or processors). The subject matter can be implemented on a single device or across multiple devices (for example, a client device and a server device). Devices implementing the subject matter can be connected through a wired and/or wireless network. Such devices can receive inputs from a user (for example, from a mouse, keyboard, or touchscreen) and produce an output to a user (for example, through a display). Specific examples disclosed are provided for illustrative purposes and do not limit the scope of the disclosure.
DRAWINGS

100

Receive a request from a service representative to access a user’s account details

110

Generate a one time password (OTP) and a summary of the account details requested for access

120

Transmit the generated OTP and summary to the user

130

Authenticate the user based on the OTP

140

Provide access of the requested account details to the service representative

150

Fig. 1
Fig. 2
Fig. 3