

provider systems remain vulnerable to phishing, man-in-the-middle and other malicious attacks, particularly during username/password exchanges, which are particular targets of hackers that understand a user's tendency to use a common password across multiple platforms. Cryptographic encoding of passwords may impair, but does not eliminate, a malicious party's ability to interfere with client accounts.

SUMMARY

[0005a] According to an aspect of the present invention, there is provided a computer-implemented method, comprising: receiving, by a service provider system, a request to access a website from a first computing device, the request comprising identifying information to identify a user of the website; sending, by the service provider system, an authentication request to a second computing device associated with the user; receiving, by the service provider system, encrypted authentication information from the second computing device, wherein the encrypted authentication information is retrieved by the second computing device from a contactless card; authenticating, by the service provider system, the encrypted authentication information based on authenticated information for the user and successfully decrypting the encrypted authentication information; and responsive to authenticating the encrypted authentication information, permitting, by the service provider system, the first computing device to access the website.

[0005b] According to another aspect of the present invention, there is provided a service provider system, comprising one or more servers comprising memory comprising instructions; and one or more processors coupled with the memory, the one or more processors, when processing the instructions, to: process a request to access a website received from a first computing device, the request comprising identifying information to identify a user of the website; cause communication of an authentication request to a second computing device associated with the user; process encrypted authentication information received from the second computing device, wherein the encrypted authentication information is retrieved by the second computing device from a contactless card; authenticate the encrypted authentication information based on authenticated information for the user and successfully decrypting the encrypted authentication information; and responsive to authenticating the encrypted authentication information, permit the first computing device to access the website.

[0005c] According to another aspect of the present invention, there is provide a computer-implemented method, comprising: receiving, by a system, a request to access an

account from a computing device, the request comprising identifying information to identify a user associated with the account; sending, by the system, an authentication request to the computing; receiving, by the system, encrypted authentication information from a contactless card via the computing device, wherein the encrypted authentication information is received by the computing device from the contactless card and communicated to the system; authenticating, by the system, the encrypted authentication information based on authenticated information for the user and successfully decrypting the encrypted authentication information; and responsive to authenticating the encrypted authentication information, permitting, by the system, the computing device to access the account.

[0006] According to the disclosure, a method for authorizing accesses to applications by clients includes the steps of: receiving a request to access an application from a first client device; identifying a client associated with the first client device; validating authenticity of the request by forwarding a notification of the request to a second client device associated with the client; receiving a response from the second client device, the response including authentication information including a username and a dynamic password retrieved by the second client device from a contactless card associated with the client. The method also includes comparing the username and dynamic password retrieved by the second client device against an expected username and expected dynamic password for the client. The method also includes responsive to a match between the username and the expected username and the dynamic password and the expected dynamic password, authenticating the request and launching the application at the first client device. The method also includes updating and storing the dynamic password associated with the client. Other embodiments of this aspect include corresponding computer systems, apparatus, and computer programs recorded on one or more computer storage devices, each configured to perform the actions of the methods.

[0007] According to the disclosure, a system for controlling accesses to applications by clients includes: a processor; an interface configured to receive an authentication request from a second client device associated with a client to authenticate an access request, made by a first client device associated with the client, for access to an application, the authentication request including a cryptogram provided by a contactless card to the second client device, the cryptogram including a username and a dynamic password; a non-transitory storage medium including a client table including at least one entry for at least one client, the at least one entry including an expected username and an

expected dynamic password for the client; program code stored on the non-transitory storage medium and operable when executed upon by the processor to:. The system also includes selectively approve the authentication request in response to a first match between the username and the expected username and to a second match between the dynamic password and the expected dynamic password. The system also includes in response to an approval of the authentication request, updating the expected dynamic password for the client. Other embodiments of this aspect include corresponding computer systems, apparatus, and computer programs recorded on one or more computer storage devices, each configured to perform the actions of the methods.

[0008] According to the disclosure, a method for authorizing access to an application by a client includes the steps of: receiving a request to access an application from a first device associated with a client; identifying the client associated with the first device; validating authenticity of the request by forwarding a notification of the request to a second device associated with the client including generating a prompt for display on the second device requesting an authentication input from the client; receiving the authentication input from the second device, the authentication input including one or more of a biometric input, a query input and a contactless card cryptogram token input including a username and dynamic password retrieved by the second device from a contactless card associated with the client. The method also includes comparing the authentication input against expected authentication input for the client. The method also includes responsive to a match between the authentication input and the expected authentication input, enabling access to the application by the first device. Other embodiments of this aspect include corresponding computer systems, apparatus, and computer programs recorded on one or more computer storage devices, each configured to perform the actions of the methods.

[0009] According to the disclosure, a method for launching applications hosted by a service provider includes the steps of registering a client with an application and binding a contactless card to the client. In one embodiment, binding the contactless card to the client may include retrieving a cryptogram comprising a username and a dynamic password from the contactless card, authenticating the username and dynamic password pair, associating the username and dynamic password pair with the client and storing the username and dynamic password pair for the client in memory. The method further

includes updating an application interface of the client to provide a contactless card login option as part of a modified application interface.

[0010] According to the disclosure, a system for launching applications includes a client interface adapted to exchange information with one or more coupled client devices, a storage device, and a table stored in the storage device and comprising an entry for at least one client, the entry including a card identifier and a dynamic card password for the client. The system includes an authentication unit, coupled to the client interface and the table, to selectively authenticate the client in response to a comparison between the card identifier and dynamic card password stored in the table and an authentication card identifier and an authentication password retrieved from a contactless card of the client. The system may also include application launch control, coupled to the authentication unit and configured to selectively launch the application for the client in response to the selective authentication of the client.

[0011] According to the disclosure, a method for launching an application includes the step of displaying a plurality of login options to a user operating a client device, the plurality of login options including a contactless card login option. The method includes, in response to selection of the contactless card login options, prompting the user to engage a contactless card with the client device to retrieve an encoded cryptogram from a storage device of the contactless card, the encoded cryptogram comprising a username and dynamic password and forwarding the encoded cryptogram to an authorization server to enable comparison of the username and the dynamic password to an expected username and an expected password for selective authentication. The method includes the step of receiving an authentication result from the authorization server and selectively launching the application in response to the authentication result.

[0012] With such an arrangement, a contactless card cryptogram exchange, which alone provides dual factor validation (knowledge of a username, dynamic password, ownership of contactless card, mobile device, etc.), may be used as a first factor authentication mechanism in a layered security protocol, thereby decreasing the potential for misappropriation of sensitive client information during client/server communications.

CLAIMS

1. A computer-implemented method, comprising:
 - receiving, by a service provider system, a request to access a website from a first computing device, the request comprising identifying information to identify a user of the website;
 - sending, by the service provider system, an authentication request to a second computing device associated with the user;
 - receiving, by the service provider system, encrypted authentication information from the second computing device, wherein the encrypted authentication information is retrieved by the second computing device from a contactless card;
 - authenticating, by the service provider system, the encrypted authentication information based on authenticated information for the user and successfully decrypting the encrypted authentication information; and
 - responsive to authenticating the encrypted authentication information, permitting, by the service provider system, the first computing device to access the website.
2. The computer-implemented method of claim 1, wherein the encrypted authentication information is comprised in a cryptogram generated by the contactless card.
3. The computer-implemented method of claim 1, wherein the encrypted authentication information is generated by the contactless card with a key and a cryptographic algorithm stored on the contactless card.
4. The computer-implemented method of claim 1, wherein the encrypted authentication information is based on a user identifier and a counter value.
5. The computer-implemented method of claim 4, wherein the user identifier is a username for the website and the counter value is related to a dynamic password to access the website.

6. The computer-implemented method of claim 1, wherein the second computing device, the contactless card, or both are registered to an account associated with the user.
7. The computer-implemented method of claim 1, comprising identifying the second computing device based on an associated between the identifying information and the second computing device.
8. The computing-implemented method of claim 1, wherein the identifying information comprises a username for the website, an Internet Protocol (IP) address, an identifier associated with the first computing device, a medium access control (MAC) address, or another identifier associated with the user.
9. A service provider system, comprising:
 - one or more servers comprising:
 - memory comprising instructions; and
 - one or more processors coupled with the memory, the one or more processors, when processing the instructions, to:
 - process a request to access a website received from a first computing device, the request comprising identifying information to identify a user of the website;
 - cause communication of an authentication request to a second computing device associated with the user;
 - process encrypted authentication information received from the second computing device, wherein the encrypted authentication information is retrieved by the second computing device from a contactless card;
 - authenticate the encrypted authentication information based on authenticated information for the user and successfully decrypting the encrypted authentication information; and
 - responsive to authenticating the encrypted authentication information, permit the first computing device to access the website.

10. The service provider system of claim 9, wherein the encrypted authentication information is comprised in a cryptogram generated by the contactless card.
11. The service provider system of claim 9, wherein the encrypted authentication information is generated by the contactless card with a key and a cryptographic algorithm stored on the contactless card.
12. The service provider system of claim 9, wherein the encrypted authentication information is based on a user identifier and a counter value.
13. The service provider system of claim 12, wherein the user identifier is a username for the website and the counter value is related to a dynamic password to access the website.
14. The service provider system of claim 9, wherein the second computing device, the contactless card, or both are registered to an account associated with the user.
15. The service provider system of claim 9, wherein the instructions are further configured to cause the one or more processors to identify the second computing device based on an associated between the identifying information and the second computing device.
16. The service provider system of claim 9, wherein the identifying information comprises a username for the website, an Internet Protocol (IP) address, an identifier associated with the first computing device, a medium access control (MAC) address, or another identifier associated with the user.
17. A computer-implemented method, comprising:
 - receiving, by a system, a request to access an account from a computing device, the request comprising identifying information to identify a user associated with the account;
 - sending, by the system, an authentication request to the computing;

receiving, by the system, encrypted authentication information from a contactless card via the computing device, wherein the encrypted authentication information is received by the computing device from the contactless card and communicated to the system;

authenticating, by the system, the encrypted authentication information based on authenticated information for the user and successfully decrypting the encrypted authentication information; and

responsive to authenticating the encrypted authentication information, permitting, by the system, the computing device to access the account.

18. The computer-implemented method of claim 17, wherein the encrypted authentication information is comprised in a cryptogram generated by the contactless card.

19. The computer-implemented method of claim 17, wherein the encrypted authentication information is generated by the contactless card with a key and a cryptographic algorithm stored on the contactless card.

20. The computer-implemented method of claim 17, wherein the encrypted authentication information is based on a user identifier and a counter value.