MULTI-FACTOR AUTHENTICATION PROVIDING A CREDENTIAL VIA A CONTACTLESS CARD FOR SECURE MESSAGING

CROSS-REFERENCE TO REATED APPLICATIONS

[0001] This application claims priority to U.S. Patent Application Serial No. 16/727,162, entitled "MULTI-FACTOR AUTHENTICATION PROVIDING A CREDENTIAL VIA A CONTACTLESS CARD FOR SECURE MESSAGING" filed on December 26, 2019 (issued as U.S. Patent No. 10,757,574 on August 25, 2020). The contents of the aforementioned patent application are incorporated herein by reference in their entirety.

BACKGROUND

[0002] Messaging services enable parties to communicate via written messages in a quick and convenient fashion. Messaging services have become increasingly used in business contexts. For example, customers may be able to have a messaging service session with a customer service representative of a company. One limitation of conventional messaging services is the lack of security. A party to a messaging service session may be able to spoof a phone number or assume a false identity in conventional messaging services sessions. As such, it is difficult to transmit potentially sensitive information, such as confidential information via conventional messaging services without fear of communicating with an imposter.

SUMMARY

[0002a] According to a first aspect of the present invention, there is provided a computing device implemented method, comprising:

receiving, by a computing system, a message from a computing device having an associated identifier, wherein the message comprises an indication to initiate a text messaging session and a cryptogram, and wherein the cryptogram comprises information to authenticate a contactless card;

decrypting, by the computing system, the cryptogram to extract the information;

authenticating, by the computing system, the information based on authenticated information stored on the computing system;

determining, by the computing system, the contactless card is associated with the identifier;

initiating, by the computing system, the text messaging session between the computing system and the computing device based on the information authenticated and the contactless card associated with the identifier.

[0002b] According to a second aspect of the present invention, there is provided a computing system, comprising:

one or more servers, the one or more servers comprising:

memory configured to store instructions; and

one or more processors coupled with the memory, the one or more processors configured to process the instructions, that when executed, cause the one or more processors to:

process a message received from a computing device, wherein computing device is associated with a phone number, the message comprises an indication to initiate a messaging session and a cryptogram, and the cryptogram comprises information to authenticate a user associated with a contactless card;

apply a cryptographic algorithm to decrypt the cryptogram;

compare the information with authenticated information to authenticate the user;

determine whether the information matches the authenticated information;

compare the phone number with a stored phone number for the computing device;

determine whether the phone number matches the stored phone number;

if the information matches the authenticated information and the phone number matches the stored phone number, initiate the messaging session with the computing device; and

if the information does not match the authenticated information or the phone number does not match the stored phone number, prevent the messaging session with the computing device.

[0002c] According to a third aspect of the present invention, there is provided a computer-implemented method, comprising:

sending, by a computing device, a message to a computing system, the message comprising a identifier to identify the computing device and an indication to establish a messaging session between the computing device and the computing system;

initiating, by the computing device via a near-field communication (NFC) interface, an NFC exchange with a contactless card;

receiving, by the computing device, a cryptogram from the contactless card in an NFC communication of the NFC exchange;

sending, by the computing device, the cryptogram to the computing system, wherein the computing system is configured to authenticate a user associated with the computing device based on the identifier and the cryptogram to establish the messaging session; and

establishing, by the computing device, the messaging session with the computing system based on a successful authentication of the identifier and the cryptogram.

[0003] There is disclosed a computing device implemented method is performed. Per this method, a message is received at a computing device from a Short Message Service (SMS) capable device having an associated phone number. The message indicates a desire to initiate an SMS session, and the message includes a secure component. The secure component is decrypted to obtain a hash of at least a onetime password and an account identifier. The onetime password and the account identifier are extracted. A determination is made whether the onetime password is valid. The account associated with the account identifier is determined, and a phone number connected with the determined account is determined. A determination is made whether the associated phone number is a matching phone number that matches the phone number connected with the account. Where the password is valid and the associated phone number is a matching phone number, a secure SMS session is initiated by sending an SMS message to the SMS capable device. Where the password is not valid and/or the associated password is not a matching phone number, the initiation of the secure SMS session with the SMS capable device is rejected.

[0004] The decrypting may use a symmetric decryption algorithm. The method may include the additional steps of checking a geolocation of the SMS-capable device and using the geolocation

as another authentication factor in determining whether or not to initiate the secure SMS session. The receiving the message may comprise receiving an SMS message. The onetime password may be a time-based password. The computing device may maintain a counter and may use a value of the counter in determining whether the password has expired. The counter maintained by the computing device may be in synch with a counter maintained by the contactless card.

[0005] There is disclosed a Short Message Service (SMS) capable device-implemented method is performed. Per this method, a cryptographically secure onetime password is received from a contactless card at the SMS capable device via a near field communication. The cryptographically secure onetime password comprises an encrypted hash of at least the onetime password and an account identifier. The onetime password is encrypted by a symmetric encryption algorithm, and the onetime password is valid for only a set period of time. A message is sent from the SMS capable device to a party to request initiation of a secure SMS session, wherein the message includes the cryptographically secure onetime password and wherein the SMS capable device has an associated phone number. Where the password is valid and where the phone number of the SMS capable device is associated with an account identified by the account identifier, an SMS message is received from the party at the SMS capable device. Where the secure SMS session is initiated, a chatbot may be used to participate in the secure SMS session.

[0006] The sending of the message from the SMS capable device may comprise sending an initial SMS message. The sending of the message from the SMS capable device may comprise one of sending the message to a website for the party or sending the message directly to the party. The method may further include sending geolocation information from the SMS capable device to the party. The SMS message may be received from a chatbot.

[0007] There is disclosed a method is performed by a contactless card. Per this method a near field communication (NFC) session is initiated with a computing device. As part of the NFC session, the contactless card communicates with an application program running on the computing device and at least a onetime password and an account identifier are passed through a hash function to create a hash value. The hash value is encrypted. The encrypted hash value is passed to the application running on the computing device. The application is prompted to send a message to a remote computing device to initiate a messaging session with the remote computing device where the message includes the encrypted hash value as evidence of an identity of a party that wishes to initiate the messaging session.

[0008] The onetime password may be a time-based password. The contactless card may maintain a counter, and a value of the counter may be used in creating the encrypted hash value. The value of the counter may be passed through the hash function. In some instances, the value

CLAIMS

1. A computing device implemented method, comprising:

receiving, by a computing system, a message from a computing device having an associated identifier, wherein the message comprises an indication to initiate a text messaging session and a cryptogram, and wherein the cryptogram comprises information to authenticate a contactless card;

decrypting, by the computing system, the cryptogram to extract the information;

authenticating, by the computing system, the information based on authenticated information stored on the computing system;

determining, by the computing system, the contactless card is associated with the identifier;

initiating, by the computing system, the text messaging session between the computing system and the computing device based on the information authenticated and the contactless card associated with the identifier.

2. The method of claim 1, wherein the decrypting uses a symmetric decryption algorithm.

3. The method of claim 1, wherein the text messaging session is a Short Message Service (SMS) messaging session, and receiving the message comprises receiving an SMS message.

4. The method of claim 1, comprising utilizing a chatbot of the computing system to communicate with the computing device in the text messaging session.

5. The method of claim 1, comprising:

performing, by the computing system, a first factor authentication to authenticate a user of the computing device based on the identifier and an authenticated identifier associated with the computing device; and

performing, by the computing system, a second factor authentication to authenticate the user of the computing device based on the information and the authenticated information.

6. The method of claim 1, wherein the identifier comprises a phone number associated with the computing device.

7. The method of claim 1, wherein the authentication information comprises a password at least partially based on cryptographic algorithm applied to a counter value by the contactless card.

8. The method of claim 1, comprising authenticating, by the computing system, a geolocation of the computing device based on the message prior to initiating the messaging session.

9. A computing system, comprising:

one or more servers, the one or more servers comprising:

memory configured to store instructions; and

one or more processors coupled with the memory, the one or more processors configured to process the instructions, that when executed, cause the one or more processors to:

process a message received from a computing device, wherein computing device is associated with a phone number, the message comprises an indication to initiate a messaging session and a cryptogram, and the cryptogram comprises information to authenticate a user associated with a contactless card;

apply a cryptographic algorithm to decrypt the cryptogram;

compare the information with authenticated information to authenticate the user;

determine whether the information matches the authenticated information;

compare the phone number with a stored phone number for the computing device;

determine whether the phone number matches the stored phone number;

if the information matches the authenticated information and the phone number matches the stored phone number, initiate the messaging session with the computing device; and

if the information does not match the authenticated information or the phone number does not match the stored phone number, prevent the messaging session with the computing device.

10. The computing system of claim 9, wherein the decrypting uses a symmetric decryption algorithm.

11. The computing system of claim 9, wherein the messaging session is a Short Message Service (SMS) messaging session, and receiving the message comprises receiving an SMS message.

12. The computing system of claim 9, further comprising instructions to cause the one or more processors to execute a chatbot, and wherein the messaging session is established between the chatbot and the computing device.

13. The computing system of claim 9, wherein the authentication information comprises a password at least partially based on cryptographic algorithm applied to a counter value by the contactless card.

14. The computing system of claim 9, further comprising instructions to cause the one or more processors to authenticate a geolocation of the computing device based on the message prior to initiating the messaging session.

15. A computer-implemented method, comprising:

sending, by a computing device, a message to a computing system, the message comprising a identifier to identify the computing device and an indication to establish a messaging session between the computing device and the computing system;

initiating, by the computing device via a near-field communication (NFC) interface, an NFC exchange with a contactless card;

receiving, by the computing device, a cryptogram from the contactless card in an NFC communication of the NFC exchange;

sending, by the computing device, the cryptogram to the computing system, wherein the computing system is configured to authenticate a user associated with the computing device based on the identifier and the cryptogram to establish the messaging session; and

establishing, by the computing device, the messaging session with the computing system based on a successful authentication of the identifier and the cryptogram.

16. The method of claim 15, wherein the messaging session is a Short Message Service (SMS) messaging session, and sending the message comprises sending an SMS message.

17. The method of claim 15, wherein the messaging session is established with a chatbot of the computing system.

18. The method of claim 15, wherein the identifier comprises a phone number associated with the computing device.

19. The method of claim 15, wherein the cryptogram comprises a password at least partially based on cryptographic algorithm applied to a counter value by the contactless card.

20. The method of claim 15, further comprising sending geolocation information to the computing system to perform an additional authentication of the user.