Secure Messaging Using Outband Mode Authentication

Field of Invention

[0001] The present invention relates to secure messaging using outband mode authentication. In particular, the invention relates to a method and system for more secure messaging by providing a plug-in to a messaging application in which each outband mode forms a factor of increasing the security of transmission of a confidential message without relying on third party servers for registration, certification or authentication.

Background

[0002] Secure electronic communication is important, especially now when messaging or sending of electronic mail is convenient and pervasive. To ensure secure messaging, messages and electronic data are often encrypted. Modern cryptographic method uses an algorithm to encrypt and decrypt messages and electronic data with a key, which may be derived from a password. For example, to use a symmetric key algorithm, a sender and recipient must have a shared or symmetric key set up in advance and kept secret from other parties; the sender uses the symmetric key for encryption whilst the recipient uses the same symmetric key for decryption.

[0003] In an asymmetric key algorithm, two keys are used. The first key is private (also known as private key) and allows a sender to encrypt data by signing; the second key is published (also known as public key) and is used for verification of signature of the sender; this provides for non-repudiation. Alternatively, the recipient's public key is used to encrypt the message and the recipient's private key is used to decrypt the encrypted message for confidentiality.

[0004] In another cyrptographic method, an algorithm encrypts a challenge identifier in a message. An encrypted challenge message is sent to a recipient. In response, the recipient's device decrypts the encrypted challenge message and encrypts the challenge identifier as a return challenge identifier in a return encrypted message. The sender's

device decrypts the return message and verifies that the return challenge identifier matches the challenge identifier to establish that communications are secure.

[0005] In conventional electronic communication, a third party server is often involved; any message or data routed through the server is susceptible to prying eyes. In the above cryptographic methods, a certification authority (CA) or vendor may be involved to issue a security certificate or license to each user; a user would have to subscribe to the CA or vendor. These security certificates or licenses have expiry dates, and must be managed by a user. In addition, a security certificate or license can be revoked. The use of a third party certification or authentication introduces procedural complexity in certificate management.

[0006] In another approach, US patent no. 5,751,814, assigned to Veritas Technology Solutions Ltd, discloses concatenating an encrypted text of a message with a password to the end of a decryption application to produce a combined file. The combined file is then converted to an electronic mail for sending to a recipient. To decrypt the sent message, the combined file is de-concatenated into its constituents and the password is used to decrypt the encrypted text. This approach is insecure because the combined file contains the password; further, the combined file and the password are in the same communication channel.

[0007] In another approach, US patent no. 6,728,378, assigned to Eversystems Information Comircio, et al, discloses sending an encrypted message and a corresponding decryption program to a recipient. The entry of a password for the program to generate a key for decrypting the encrypted message ensures integrity and authenticity of the sent and received messages.

[0008] Despite development in making transmission of messages more secure, it can thus be seen that there exists a need to provide another method and system for secure messaging.

Summary

[0009] The following presents a simplified summary to provide a basic understanding of the present invention. This summary is not an extensive overview of the invention, and is not intended to identify key features of the invention. Rather, it is to present some of the inventive concepts of this invention in a generalised form as a prelude to the detailed description that is to follow.

[0010] In one embodiment, the present invention provides a secure messaging system. The secure messaging system comprises: a security module pluggable into a messaging application and associated with a messaging device; wherein said messaging device has first and second input/output (I/O) channels; and wherein a secure message is operable to be sent to a recipient via the first I/O channel, with the security module allowing the sender to encrypt the secure message with a key generated by a passphrase, to split the passphrase into sub-passphrases and to send at least one of the sub-passphrases to the recipient via the second I/O channel, which is out-of-band with the first I/O channel.

[0011] In another embodiment, the present invention provides a method for sending and receiving a secure message. The method comprises: encrypting the message with a key generated by a passphrase before sending the message via an input/output channel; splitting the passphrase into sub-passphrases; sending at least one sub-passphrase via an outband channel, which is separate from the I/O channel for sending the message; and receiving the sub-passphrases and re-assembling the sub-passphrases to form the passphrase, which is operable to generate a key for decrypting the secure message received.

[0012] In another embodiment, the present invention provides a computer readable medium. The medium comprises a security module that is pluggable into a messaging application, wherein the security module allows a sender to encrypt a secure message with a key generated by a passphrase, to split the passphrase into sub-passphrases and to send one of the sub-passphrases to a recipient via an out-of-band channel, which is separate from an input/output channel for communicating the secure message to the recipient.

[0013] In another embodiment of the present invention, the security module comprises a protocol for sending and receiving the passphrase or sub-passphrases. In one embodiment, the protocol generates a settings interface for defining a mode for sending the passphrase or a combination of modes for sending the sub-passphrases. In another embodiment, the settings interface is associated with an instant messenger. In another embodiment, the settings interface is associated with an email application and the settings interface further comprises SMTP and POP3 setting boxes. In yet another embodiment, the settings interface is associated with SMS and the settings interface further comprises gateway and gateway password setting boxes.

[0014] In another embodiment, the protocol defines and identifies the order of the sub-passphrases. The sub-passphrases may be sent successively or simultaneously.

[0015] In yet another embodiment of the present invention, encryption or decryption of the secure message is carried out with a symmetric cryptographic algorithm.

Brief Description of the Drawings

[0016] This invention will be described by way of non-limiting embodiments of the present invention, with reference to the accompanying drawings, in which:

[0017] FIG. 1 illustrates an architecture of a secure messaging system according to an embodiment of the present invention;

[0018] FIG. 2 illustrates an instant messaging settings interface according to another embodiment of the present invention;

[0019] FIG. 3 illustrates a process flow according to another embodiment of the present invention;

[0020] FIG. 4 illustrates an email messaging settings interface according to another embodiment of the present invention; and

[0021] FIG. 5 illustrates a short message service settings interface according to yet another embodiment of the present invention.

Detailed Description

[0022] One or more specific and alternative embodiments of the present invention will now be described with reference to the attached drawings. It shall be apparent to one skilled in the art, however, that this invention may be practised without such specific details. Some of the details may not be described at length so as not to obscure the invention. For ease of reference, common reference numerals or series of numerals will be used throughout the figures when referring to the same or similar features common to the figures.

[0023] FIG. 1 shows a secure messaging architecture according to an embodiment of the present invention. The secure messaging system 100 includes a number of messaging devices 110; these messaging devices 110 are in communication, for example, through the internet or an intranet. FIG. 1 shows two such messaging devices 110, 110a that are in communication through the internet 50. Each messaging device 110,110a has a messaging application 120,120a; a security module 130,130a; and a processor 140,140a. Each messaging device 110,110a is configured with two input/output (I/O) channels 150,160. As shown in FIG. 1, the first I/O channel 150 allows the messaging device 110,110a to connect to the internet 50 for sending a message to a recipient, for example, via emailing 151, instant messaging 152, short message service (SMS) 153, and so on, whilst the second I/O channel 160 allows the security module 130,130a to send a passphrase 134 (including a password) or a sub-passphrase of the passphrase 134 to the recipient. As shown in FIG. 1, the second I/O channel 160 is connected to a network card 162,162a; a modem 164,164a; and/or a facsimile/modem 166,166a. In other words, the second I/O channel 160 is used to send the passphrase 134 to the recipient via one or more modes of the second I/O channel

160, such as, email, short message service (SMS), instant messaging, internet phone/VoIP, telephone, facsimile, and so on. In this invention, the second I/O channel 160, which is separate from the first I/O channel 150 for sending the message, is used by a sender for sending out a passphrase 134 to a recipient; the second I/O channel 160 is thus referred to as an out-of-band or outband channel 160.

[0024] In one embodiment of the present invention, the network card 162,162a is configured to connect to the internet 50. In another embodiment of the present invention, the modem 164,164a is configured to connect to the internet 50 via a public switched telephone network (PSTN) or broadband 70, the modem 164,164a allows a user to communicate via email, instant messaging or telephone. In yet another embodiment of the present invention, the facsimile/modem 166,166a is connected directly to a PSTN; the facsimile/modem 166,166a allows a user to communicate via email, instant messaging, telephone or facsimile; in another embodiment, the PSTN is a mobile telephone gateway. With the present invention, when a confidential message is sent through the I/O channel 150 via, for example, an instant messaging application 120,120a, the security module 130,130a allows a sender to send a passphrase 134 or a sub-passphrase 134a,134b, etc. via an outband channel 160 that is separate from the I/O channel 150 for sending the message to the recipient.

[0025] In one embodiment of the security module, the security module 130,130a is a software module that is pluggable into one's messaging application. The security module 130,130a thus allows a user to enhance a cryptographic algorithm 80, that has been added into one's messaging application, by sending a passphrase 134 to a recipient via the outband channel 160. In one embodiment, the cryptographic algorithm 80 is a symmetric key cryptographic algorithm, such as the Advanced Encryption Standard (AES). In another embodiment of the security module, the security module 130,130a includes a protocol 132. The protocol 132 allows a user to enter a passphrase 134, instead of a simple password, and also allows the passphrase 134 to be split into a predetermined number of sub-passphrases 134a,134b, etc. Each sub-passphrase 134a,134b, etc. is then communicated to the recipient successively via any one mode of the outband channel 160. During successive transmission of the sub-passphrases, the sub-passphrases may be in an order according to the order of the sub-passphrases that

constitute the passphrase, or the sub-passphrases may be in any order depending on the processor 140. In another embodiment, all the sub-passphrases are sent simultaneously through the outband channel 160 to the recipient. In another embodiment, at least one of the sub-passphrases 134a,134b is communicated to the recipient via the outband channel 160. In yet another embodiment, the sub-passphrases 134a,134b, etc. are communicated via a combination of modes of the outband channel 160. In use, the security module 130,130a and protocol 132 provide for the identification of the order of the sub-passphrases with appropriate comments, for example, "this is sub-passphrase 2 of 3".

[0026] FIG. 2 shows a dialogue box 136 generated by the security module 130,130a and according to the protocol 132. The dialogue box 136 allows a sender to enter one's passphrase 134 and to choose the mode(s) of communicating the sub-passphrases 134a,134b, etc. via the outband channel 160 to a recipient. As shown in FIG. 2, such modes of communicating the sub-passphrases may be via telephone; SMS; email; SMS and email; IM and SMS; and so on. As can be seen from FIG. 2, the dialogue box also allows a sender to choose a different mode of communicating each sub-passphrase 134a,134b, etc; for example, a user may choose to send the first sub-passphrase via SMS and the second sub-passphrase via email.

[0027] Upon receipt of the sub-passphrases 134a,134b, etc, the protocol 132 running in the recipient's messaging device 110 assembles the sub-passphrases 134a,134b,etc. electronically according to one embodiment. For example, with order sequence of each sub-passphrase defined by the protocol 132, the security module 130a re-assembles the sub-passphrases together to form the passphrase 134 before using the passphrase 134 to generate the symmetric key for decrypting the secure message that was received. In another embodiment, the protocol 132 prompts the recipient to manually enter each sub-passphrase 134a,134b, etc. in the order set by the sender to form the passphrase 134 for the cryptographic algorithm 80 to generate a symmetric key for decrypting the secure message received.

[0028] FIG. 3 shows a process flow chart according to an embodiment of the present invention. As shown in FIG. 3, a sender enters a message, in step 205, for sending it as

a secure message according to the present invention. In the sender's messaging application 120, a cryptographic algorithm 80 together with a security module 130 according to the present invention have already been plugged-in. With the protocol 132 operating in the security module 130, the sender enters a passphrase 134 into the dialogue box that has popped up in the messaging application 120. Upon entering the passphrase 134, the protocol 132 sends the passphrase 134, in step 215, to the cryptographic algorithm 80; at the same time, the protocol 132 splits, in step 220, the passphrase 134 into predetermined numbers of sub-passphrases 134a,134b, etc. before sending the sub-passphrases to the processor 140 of the sender's device 110; in response, the processor 140 sends at least one sub-passphrase 134a,134b,etc. via the outband channel 160, namely, the relevant network card 162, modem 164 and/or facsimile/modem 166. As shown in FIG. 2, at least one sub-passphrase may be sent through the network card 162 by email, instant message, SMS, VoIP, etc; through the modem 164 by email, instant message, SMS, VoIP, etc; and through a facsimile/modem 166. In parallel or in sequence to the transmission of the passphrase 134 or sub-passphrases 134a,134b,etc., the messaging application 120 sends, in step 225, the encrypted message through the I/O channel 150, for example, by email, instant message, SMS, and so on.

[0029] At the recipient's device 110a, the encrypted message is received, in step 230, by the messaging application 120a. In response, the protocol 132 in the security module 130a handshakes with the processor 140a and the I/O channel 160 to receive the sub-passphrases 134a,134b, etc. sent by the sender. The protocol 132 at the recipient's device then assembles the sub-passphrases in the correct order to form the passphrase 134, in step 240. The protocol 132 then sends the passphrase 134, in step 245, to the decryption algorithm 80; in response, the decryption algorithm 80 decrypts the encrypted message and retrieves the secure message, in step 250.

[0030] The present invention allows a user to send a secure message, for example, a confidential message, to a recipient by sending a passphrase 134 or splitting a passphrase 134 into a predetermined number of sub-passphrases 134a,134b, etc. and allowing the sender to communicate the passphrase 134 or at least one sub-passphrase 134a,134b, etc. to the recipient via the outband (second) I/O channel 160. With the

present invention, separating the passphrase channel from the messaging channel makes transmission of a message more secure. Splitting the passphrase 134 into sub-passphrases 134a,134b, etc. further increases secure transmission of the message. Sending each sub-passphrase 134a,134b, etc.via each mode of the outband channel 160 provides a factor of difficulty in re-assembling the passphrase 134 used by the sender; with each additional factor of difficulty in re-assembling the passphrase 134, the difficulty of reading the secure message is increased. In another embodiment of the present invention, the difficulty of re-assembling the passphrase for decrypting the secure message is increased by increasing the number of sub-passphrases. In yet another embodiment, the difficulty of re-assembling the passphrase is increased further by using a passphrase only once. In addition, with each transmission of the passphrase or each sub-passphrase, the protocol 132 performs a form of authentication, thereby ensuring the transmission of the confidential message is secure.

[0031] Another advantage of the present invention is that the security module 130,130a is a plug-in module that works with any messaging application, such as, instant messaging or emailing software. It involves only the users at the sender and recipient ends; in other words, it involves only the peers in communication; no intermediate processes are involved in the secure message communication of the present invention. In instant messaging, no intermediate server is also involved in the secure message communication, thus providing instant messaging with higher security by doing away with third party authentication. Another advantage of the present invention is that the security module 130,130a is a small program that is light-weight and is, therefore, easy to use. This contrasts with the complex key and certificate administration and management procedures in conventional public key infrastructure (PKI) involving a third party, which resulted in its low adoption rate.

[0032] In an implementation of the present invention, the security module 130,130a is plugged-in to an instant messenger application. For example, the Add-in or Plug-in tab in a messenger application is opened and the add-in/plug-in path(s) is/are entered. Once the paths for the security module 130,130a and cryptographic algorithm 80 are defined, clicking on an activate button adds the functionalities of the security module and cryptographic algorithm into the messenger application. A setting interface, as shown

in FIG. 2, would then appear and allow a user to define the mode(s) for sending a passphrase or sub-passphrases to a recipient.

[0033] In an implementation of the present invention for emailing, the security module 130,130a generates a setting interface 400, as shown in FIG. 4, for enhancing ease of use and settings. As shown in FIG. 4, the setting interface 400 provides an outgoing mail (or simple mail transfer protocol (SMTP)) configuration box 410 and an incoming mail (or post office protocol (POP3)) configuration box 420.

[0034] In an implementation of the present invention for SMS, the security module 130,130a generates another setting interface 500, as shown in FIG. 5. As shown in FIG. 5, the setting interface 500 provides a user a box 510 to define the SMS gateway. In addition, another user box 520 is provided for a user to enter an SMS gateway password.

[0035] While specific embodiments have been described and illustrated, it is understood that many changes, modifications, variations and combinations thereof could be made to the present invention without departing from the scope of the invention. In Microsoft Windows Live Messenger, the secure messaging mechanism of the present invention is not applied symmetrically in the incoming message algorithm and outgoing message algorithm; for example, the security module 130a is implemented using Windows Live Messenger Activity website configured by a profile setting in XML (eXtensible Markup Language) while the security module 130 is implemented as an add-in using Windows Live Messenger Add-in API (Application Programming Interface). However, the principle underlying secure messaging of the present invention for implementation in Microsoft Windows Live Messenger remains substantially the same.

CLAIMS:

1. A secure messaging system comprising:

a security module pluggable into a messaging application and associated with a messaging device;

wherein said messaging device has first and second input/output (I/O) channels; and wherein a secure message is operable to be sent to a recipient via the first I/O channel, with the security module allowing the sender to encrypt the secure message with a key generated by a passphrase, to split the passphrase into sub-passphrases and to send at least one of the sub-passphrases to the recipient via the second I/O channel, which is out-of-band with the first I/O channel.

2. A system according to claim 1, wherein the security module comprises a protocol for splitting the passphrase and sending/receiving the passphrases and sub-passphrases.

3. A system according to claim 2, wherein the protocol generates a settings interface for defining a mode for sending the passphrase or combination of modes for sending the sub-passphrases.

4. A system according to any one of the preceding claims, wherein the messaging application is an instant messenger.

5. A system according to claim 3, wherein the settings interface comprises SMTP and POP3 setting boxes when the messaging application is an email application.

6. A system according to claim 3, wherein the settings interface comprises a gateway setting box and a gateway password box when the messaging application is SMS.

7. A system according to any one of claims 2-6, wherein the protocol defines and identifies the order of the sub-passphrases.

8. A system according to any one of claims 2-7, wherein transmission of the sub-passphrases is successively.

9. A system according to any one of claims 2-7, wherein transmission of the sub-passphrases is simultaneously.

10. A system according to any one of the preceding claims, wherein encryption or decryption of the secure message is carried out with a symmetric cryptographic algorithm.

11. A method for sending and receiving a secure message, the method comprising:

encrypting a message with a key generated by a passphrase, which is entered by a sender, before sending the message via an input/output channel;

splitting the passphrase into sub-passphrases;

sending at least one sub-passphrase via an outband channel, which is separate from the I/O channel for sending the message; and

receiving the sub-passphrases and re-assembling the sub-passphrases by a recipient to form the passphrase, which is operable to generate a key for decrypting the secure message received.

12. A method according to claim 11, wherein said splitting, sending and receiving are carried out according to a protocol.

13. A method according to claim 12, wherein the protocol generates a settings interface for defining a mode or combination of modes for sending the sub-passphrases.

14. A method according to any one of claims 11-13, wherein sending and receiving the secure message is carried out by an instant messenger.

15. A method according to claim 12, wherein the settings interface comprises SMTP and POP3 setting boxes when sending the secure message is carried out by emailing.

16. A method according to claim 12, wherein the settings interface comprises gateway and gateway password setting boxes when sending the secure message is carried out by SMS.

17. A method according to any one of claims 12-16, wherein the protocol defines and identifies the order of the sub-passphrases.

18. A method according to any one of claims 11-17, wherein sending of the sub-passphrases is successively.

19. A method according to any one of claims 11-17, wherein sending of the sub-passphrases is simultaneously.

20. A method according to any one of claims 11-19, wherein encrypting or decrypting the message is carried out by a symmetric cryptographic algorithm.

21. A computer readable medium comprising:

a security module pluggable into a messaging application;

wherein the security module allows a sender to encrypt a secure message with a key generated by a passphrase, to split the passphrase into sub-passphrases and to send one of the sub-passphrases to a recipient via an out-of-band channel, which is separate from an input/output channel for communicating the secure message to the recipient.

22. A computer readable medium according to claim 21, wherein the security module further comprises a protocol for sending and receiving the passphrase or sub-passphrases.

23. A computer readable medium according to claim 21 or 22, wherein the medium further comprising a symmetric cryptographic algorithm.