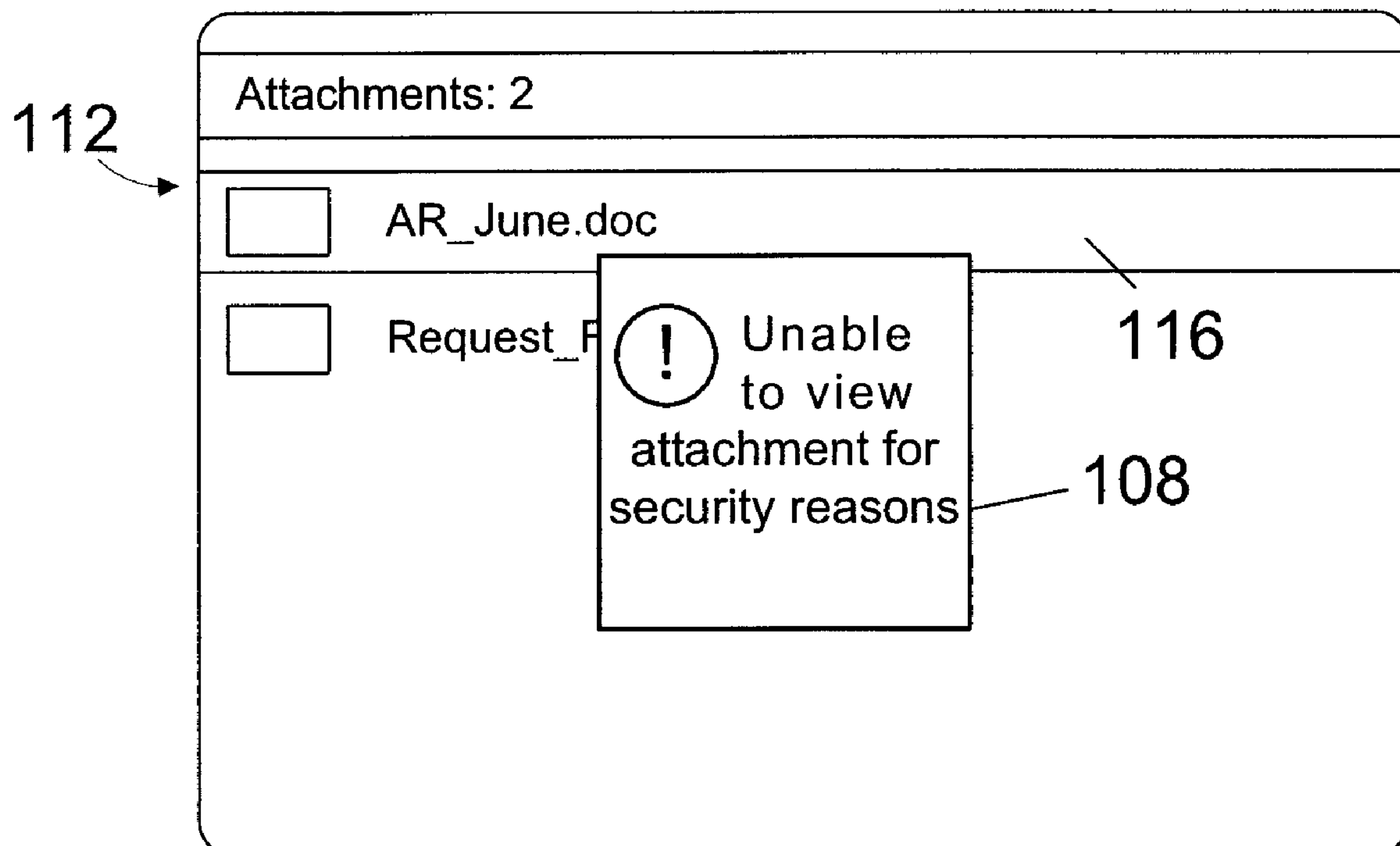




(22) Date de dépôt/Filing Date: 2006/11/23
(41) Mise à la disp. pub./Open to Public Insp.: 2007/05/23
(30) Priorité/Priority: 2005/11/23 (EP05111192.0)

(51) Cl.Int./Int.Cl. *H04L 9/00* (2006.01),
H04L 12/54 (2006.01)
(71) Demandeur/Applicant:
RESEARCH IN MOTION LIMITED, CA
(72) Inventeurs/Inventors:
BROWN, MICHAEL K., CA;
KIRKUP, MIKE, CA;
BROWN, MICHAEL S., CA
(74) Agent: RIDOUT & MAYBEE LLP

(54) Titre : COURRIEL AVEC PARTIES DE MESSAGE SECURISEES
(54) Title: E-MAIL WITH SECURE MESSAGE PARTS



(57) **Abrégé/Abstract:**

A method for preventing a recipient of an electronically transmitted message (74) from taking at least one action in relation to the message (74) is disclosed. The message (74) has at least two parts (102, 116) with one of the parts (116) having a higher level of security than the other part (102). The method includes the step of extracting information from the message (74). The information indicates that the higher level security part (116) is not permitted to have the action taken on it while the other part (102) is so permitted. The method also includes the step of preventing the higher level security part (116) from having the action taken on it in reaction to said recipient making an offending request.



ABSTRACT

A method for preventing a recipient of an electronically transmitted message (74) from taking at least one action in relation to the message (74) is disclosed. The message (74) has at least two parts (102, 116) with one of the parts (116) having a higher level of security than the other part (102). The method includes the step of extracting information from the message (74). The information indicates that the higher level security part (116) is not permitted to have the action taken on it while the other part (102) is so permitted. The method also includes the step of preventing the higher level security part (116) from having the action taken on it in reaction to said recipient making an offending request.

- 1 -

E-MAIL WITH SECURE MESSAGE PARTS**FIELD**

- 5 **[0001]** The present invention relates to e-mails that have secure message parts and, in particular, to methods and systems for keeping secure message parts of e-mails protected.

BACKGROUND

- 10 **[0002]** Handheld electronic devices are commonly used to store and display messages. Devices that are enabled for wireless communication may also be used for sending and receiving messages. Where possible, the devices have been provided with a messaging application having a user interface similar to the user interface found for similar applications on
- 15 a desktop computer. Also, some of the messaging applications that run on handheld electronic devices have mechanisms to reduce the risk of outbound e-mails having their contents exposed by way of illicit interception. Possible mechanisms include encryption software for creating encrypted e-mails.
- 20 **[0003]** In addition to encrypting e-mails, it is possible that the security risk can be reduced further by additional means. For example, through the use of PGP™ (Pretty Good Privacy) software, it is possible to mark a message so that it can only be viewed (in the PGP™ application) with a "secure" viewer. Forcing the message to be viewed in this viewer
- 25 means the message will be viewed in a tempest resistant font. A possible limitation of this PGP™ method is that it only addresses how to view certain data at the node of the message receiver.
- [0004]** Accordingly, it would be advantageous to improve methods and systems for keeping secure message parts of e-mails protected.

SUMMARY

[0005] According to one example embodiment is a method for preventing a recipient of an electronically transmitted message from taking
5 at least one action in relation to the message. The message has at least two parts with one of the parts having a higher level of security than the other part. The method includes the step of extracting information from the message. The information indicates that the higher level security part is not permitted to have the action taken on it while the other part is so
10 permitted. The method also includes the step of preventing the higher level security part from having the action taken on it in reaction to the recipient making an offending request.

[0006] According to another example embodiment is a handheld electronic device having a messaging application permitting a recipient of
15 an electronically transmitted message to take actions in relation to the message. The handheld device includes a display screen. A processor is in electronic communication with the display screen. The processor is capable of controlling operation of the display screen. At least one computer readable medium stores code and is in electronic communication
20 with the processor. The code includes computer executable instructions for extracting information from the message. The information indicates that at least a first part of the message is not permitted to have a certain action taken on it while at least a second part of the message is so permitted. The code also includes computer executable instructions for
25 preventing the first part from having the certain action taken on it in reaction to the recipient making an offending request.

[0007] According to another example embodiment is a computer program product having a computer readable medium storing a messaging application. The messaging application can process an electronically
30 transmitted message having at least two parts with one of the parts having a higher level of security than the other part. A recipient of the

- 3 -

message is prevented from taking at least one action in relation to the message. The messaging application includes code for extracting information from the message. The information indicates that the higher level security part is not permitted to have the action taken on it while the other part is so permitted. The messaging application also includes code for preventing the higher level security part from having the action taken on it in reaction to the recipient making an offending request.

BRIEF DESCRIPTION OF THE DRAWINGS

10 **[0008]** Reference will now be made, by way of example, to the accompanying drawings which show example embodiments of the present invention, and in which:

[0009] Figure 1 shows a block diagram of a user device to which the present invention can be applied in an example embodiment;

15 **[0010]** Figure 2 shows, in diagrammatic form, a first screen shot of a possible messaging application for the device of Figure 1;

[0011] Figure 3 shows, in diagrammatic form, a second screen shot of the messaging application of Figure 2, the second screen shot being that of a displayed message;

20 **[0012]** Figure 4 shows, in diagrammatic form, a screen shot taken after a person tries to open an attachment of the displayed message;

[0013] Figure 5 shows, in diagrammatic form, a screen shot illustrating a message forwarding example with a message attachment being the message part marked with one or more action restrictions in this example; and

25

[0014] Figure 6 shows, in diagrammatic form, a screen shot illustrating an alternative message forwarding example with a portion of the message body being the message part marked with one or more action

- 4 -

restrictions in this example.

[0015] Similar reference numerals may have been used in different figures to denote similar components.

5 **DESCRIPTION OF EXAMPLE EMBODIMENTS**

[0016] The following description of specific embodiments of the invention does not limit the implementation of the invention to any particular computer programming language or system architecture. The present invention is not limited to any particular operating system, mobile
10 device architecture, or computer programming language. Moreover, although some of the embodiments described below include mobile devices, the present invention is not limited to mobile devices; rather, it may be embodied within a variety of user devices or terminals, including handheld devices, mobile telephones, personal digital assistants (PDAs),
15 personal computers, audio-visual terminals, televisions, and other devices. One skilled in the art will appreciate that messaging applications can be installed on most of these user devices and terminals.

[0017] Any references herein to "messages" are not intended to be limited to e-mail, but should be understood to include other types of
20 messages that one skilled in the art would understand to be possible in the context in which the term is being used. Other types of messages include text messages, audio messages, video messages, and other items, including calendar entries, tasks, and other date-related items.

[0018] Referring now to the drawings, Figure 1 is a block diagram of
25 a user device to which the present invention can be applied in an example embodiment. In the example embodiment, the user device is a two-way mobile communication device 10 having data and possibly also voice communication capabilities. In an example embodiment, the device 10 has the capability to communicate with other computer systems on the
30 Internet. Depending on the functionality provided by the device 10, in

- 5 -

various embodiments the device may be a data communication device, a multiple-mode communication device configured for both data and voice communication, a mobile telephone, a PDA enabled for wireless communication, or a computer system with a wireless modem, among
5 other things.

[0019] In the illustrated embodiment, the device 10 includes a communication subsystem 11. In one embodiment, the communication subsystem 11 may include a receiver, a transmitter, and associated components such as one or more, preferably embedded or internal,
10 antenna elements, and a processing module such as a digital signal processor (DSP). As will be apparent to those skilled in the field of communications, the particular design of the communication subsystem 11 will be dependent in part upon the communication network in which the device 10 is intended to operate.

15 **[0020]** Signals received by the device 10 from a wireless communication network 50 are input to the receiver of the communication subsystem 11, which may perform such common receiver functions as signal amplification, frequency down conversion, filtering, channel selection and the like. In a similar manner, signals to be transmitted are processed,
20 including modulation and encoding for example, by the DSP and input to the transmitter for digital to analog conversion, frequency up conversion, filtering, amplification and transmission over the wireless communication network 50.

[0021] The device 10 includes a microprocessor 38 that controls the
25 overall operation of the device. The microprocessor 38 interacts with the communications subsystem 11 and also interacts with further device subsystems such as a graphics subsystem 44, flash memory 24, random access memory (RAM) 26, auxiliary input/output (I/O) subsystems 28, serial port 30, keyboard or keypad 32, speaker 34, microphone 36, a
30 short-range communications subsystem 40, and any other device subsystems generally designated as 42. The graphics subsystem 44 interacts with the display 22 and renders graphics and/or text upon the

- 6 -

display 22.

[0022] Operating system software 54 and various software applications 58 used by the microprocessor 38 are, in one example embodiment, stored in a persistent store such as flash memory 24 or similar storage element. Those skilled in the art will appreciate that the operating system 54, software applications 58, or parts thereof, may be temporarily loaded into a volatile store such as RAM 26. It is contemplated that received communication signals may also be stored to RAM 26.

[0023] The microprocessor 38, in addition to its operating system functions, can enable execution of software applications 58 on the device. A predetermined set of software applications 58 which control basic device operations, including data and voice communication applications for example, will normally be installed on the device 10 during manufacture. Further software applications 58 may also be loaded onto the device 10 through the network 50, an auxiliary I/O subsystem 28, serial port 30, short-range communications subsystem 40 or any other suitable subsystem 42, and installed by a user in the RAM 26 or a non-volatile store for execution by the microprocessor 38. Such flexibility in application installation increases the functionality of the device and may provide enhanced on-device functions, communication-related functions, or both. For example, secure communication applications may enable electronic commerce functions and other such financial transactions to be performed using the device 10.

[0024] In a data communication mode, a received signal such as a text message or web page download will be processed by the communication subsystem 11 and input to the microprocessor 38, which will preferably further process the received signal for output to the display 22 through the graphics subsystem 44, or alternatively to an auxiliary I/O device 28. A user of device 10 may also compose data items within a software application 58, such as e-mail messages for example, using the keyboard 32 in conjunction with the display 22 and possibly an auxiliary I/O device 28 such as, for example, a thumbwheel. Such composed items

- 7 -

may then be transmitted over a communication network through the communication subsystem 11.

[0025] The serial port 30 in Figure 1 would normally be implemented in a personal digital assistant (PDA)-type communication device for which
5 synchronization with a user's desktop computer (not shown) may be desirable, but is an optional device component. Such a port 30 would enable a user to set preferences through an external device or software application and would extend the capabilities of the device by providing for information or software downloads to the device 10 other than through a
10 wireless communication network.

[0026] A short-range communications subsystem 40 is a further component which may provide for communication between the device 10 and different systems or devices, which need not necessarily be similar devices. For example, the subsystem 40 may include an infrared device
15 and associated circuits and components or a Bluetooth™ communication module to provide for communication with similarly enabled systems and devices. The device 10 may be a handheld device.

[0027] Wireless mobile network 50 is, in an example embodiment, a wireless packet data network, (e.g. Mobitex™ or DataTAC™), which
20 provides radio coverage to mobile devices 10. Wireless mobile network 50 may also be a voice and data network such as GSM (Global System for Mobile Communication) and GPRS (General Packet Radio System), CDMA (Code Division Multiple Access), or various other third generation networks such as EDGE (Enhanced Data rates for GSM Evolution) or UMTS
25 (Universal Mobile Telecommunications Systems). In some example embodiments, network 50 is a wireless local area network (WLAN) operating, for example, in conformance with one or more IEEE 802.11 protocols. In some example embodiments, the device 10 is configured to communicate over both wireless wide area networks and wireless local area
30 networks.

[0028] In one embodiment, the software resident on the device 10

- 8 -

includes a messaging application 56 for sending, receiving and displaying messages or other items, such as tasks, calendar items, etc. An example of a very well known software application similar to the messaging application 56 is the Microsoft Outlook™ software application produced by the Microsoft Corporation. There exists a variety of publications that provide instructions for developing and creating messaging applications. Furthermore, software is currently available for building messaging applications. Accordingly, code-level programming specifics need not be described herein in order for one skilled in the art to build a messaging application having any of the functionality disclosed herein. Associated with the messaging application 56 is an e-mail security module 57 for configuring the device 10 to perform at least some of the e-mail security functions described herein. In the presently described embodiment, module 57 is a sub-component of messaging application 56, however in alternative embodiments all or portions of module 57 may be part of another software application or may be a separate software application.

[0029] It is again noted that the present application is not limited to use in association with e-mail messages and may apply to other messages where possible, including SMS messages, and other "items", including calendar entries, task list entries, and other items having a date associated with them. References in the present application to "messages" or a "messaging application" should be understood to encompass and include possibilities within this wider range of items.

[0030] Referring to Figure 2, a screen shot 70 generated by an example embodiment of the messaging application 56 is illustrated. The screen shot 70 corresponds to what the display of a mobile communication device might look like after a user has requested that the messaging application 56 display received messages in a list. This is typically done by clicking on an icon or a particular list selection associated with a request to display inbox folder contents.

[0031] In the screen shot 70, a plurality of messages 74 are listed vertically. Going from left to right in the screen shot 70, there is a

- 9 -

message icon column 78, a sender identifier column 82 and a message subject column 86. Icons 88 in the icon column 78 can provide information about the e-mails with which they are associated. For example, an icon 88 associated with an e-mail that has already been read
5 can provide this information to the user by means of an appropriate graphical image displayed to the user (e.g. an envelope with its flap opened). Similarly an appropriate graphical image could be used for an e-mail that has not been read (e.g. an envelope with its flap closed). The columns 82 and 86 also provide information about the messages 74. In
10 the column 82, the names of the people who sent the e-mails 74 are listed. In the column 86, the subject lines of the e-mails 74 are shown.

[0032] It will be understood that the display of the mobile communication device could show additional/fewer and/or different columns than those shown in Figure 2. Some examples of alternative
15 columns are importance, flag status, presence of attachment(s), received date, and message size. Due to the typical width of the display of a mobile communication device, it will normally not be desirable to have a large number of columns, and it will normally be desirable to show the columns that provide the most useful information keeping in mind that the user is
20 probably looking for a particular message at the stage shown in Figure 2.

[0033] Message 90 of the messages 74 has been highlighted by the user. The sender of the message 90 is Accounting, and the subject line of the message is "AR Reports". The user in this example now requests, using one or more of the input devices of his mobile communication
25 device, that the message 90 be opened.

[0034] Figure 3 is a screen shot 94 of the displayed message 90. Message header 98 repeats the information of the message 90 contained in the columns 82 and 86 of the screen shot 70. It will be understood that the header 98 could show additional/less and/or different information than
30 what is shown. Below the header 98 is a message section 102 that contains the text of the message, and the section 102 is commonly referred to as the message body. Below the message body 102 is a

- 10 -

section 104 providing a description of two attachments to the message 90. The message 90 has three parts. One of the parts is the text of the message, and the other two parts are the two attachments.

[0035] In the present example, the user reads the message body
5 102. From reading the message body 102, the user learns that Jane Doe in accounting has sent him two files, in particular, two Word™ documents. Assuming the user is reading the message from top to bottom, the user then learns (after reading the section 104) that the two Word™ documents that Jane Doe has sent him are "AR_June.doc" and "Request_form.doc".

10 **[0036]** In the present example, the message body 102 and the two documents listed in the section 104 were encoded in the Multipurpose Internet Mail Extension (MIME) standard during the process by which the message was sent. MIME is an official Internet standard that specifies how
15 messages should be formatted so that they can be exchanged between different message systems. MIME is also a specification for the format of non-text message attachments that allows the attachment to be sent over the Internet.

[0037] In the illustrated example, the conversion of attachments (such as the two attachments in the example e-mail) from MIME to files or
20 vice versa is normally handled by the messaging application 56 (Figure 1). When the file is stored on the device 10, it is up to the operating system 54 to map one of the applications 58 to the file type.

[0038] When a MIME formatted message is processed by the messaging application 56, information is extracted from the message.
25 Many different types of information can be extracted from messages, and some examples of possible types of extractable information are the content types in the message, body parts, how the message data is encoded, the version of the MIME standard that the message conforms to, the sender of the message, and the date and time the message was sent. Also, one
30 skilled in the art will appreciate that information can be extracted from MIME attributes of a message.

- 11 -

[0039] Continuing on with the example message from Accounting to the next screen shot shown in Figure 4, the messaging application 56 in this example embodiment offers the user the ability to proceed to a screen where the attachments of the message 90 are listed for selection. At this stage the screen is as illustrated in screen shot 112, except initially without dialog window 108. In the screen shot 112, message attachment 116, which is "AR_June.doc", is highlighted and ready for selection. (It will be kept in mind that the ways in which a user opens the attachments of a message vary depending on the messaging application. In some messaging applications, message attachments are opened by clicking on icons in the message body).

[0040] It will be understood that in some messaging system architectures within which the device 10 can operate, the example received message may require, when at least some parts of the message need to be reviewed, the outbound sending of these message parts through the communications subsystem 11 (Figure 1) to an attachment server. The purpose of the attachment server being that it formats and/or decodes various message parts for viewing on the device. This procedure however might have the potential of compromising intended level of security because there could be transmission of one or more message parts in a decoded (or unsatisfactorily coded) format over a public network during this procedure. For these example embodiments, the use of MIME attributes in relation to the message parts could enable prevention of undesired transmission of message parts to servers such as an attachment server.

[0041] Taking the message attachment 116 as an example, the user attempts to use one or more of the input devices of his mobile communication device to open the message attachment 116. The messaging application however has processed a MIME attribute which the messaging application interprets to mean that the attachment will not be sent off of the device. In this example, the attachment is not to be displayed to the user because it cannot be sent to the attachment server for decoding as a result of the attachment's MIME attribute being

- 12 -

"Content-Forwarding: denied". Conversely, the attachment would, in this example, be permitted to be sent to the attachment server, and thus could be displayed to the user if its MIME attribute was "Content-Forwarding: allowed".

5 **[0042]** Thus, for the above example, the message attachment 116 is not decoded for viewing on the device. Instead the dialog window 108 informs the user that the message attachment 116 cannot be viewed due to security reasons.

10 **[0043]** It will be understood that there are a variety of alternative ways in which the user could be made aware that his request offends a security precaution and that the message attachment 116 cannot be viewed. For example, there could simply be a beep that sounds when the user requests to open the message attachment 116.

15 **[0044]** Still with reference to the example message from Accounting, Figure 5 is a screen shot 124 illustrating a forwarded message composition derived from the original message 90. It will be understood that the request by the device user in this example to forward a message can in fact be viewed as a bundle of requests including a request to forward the message text, a request to forward the "AR_June.doc" attachment and a
20 request to forward the "Request_Form.doc" attachment.

25 **[0045]** As indicated in message header 128, the forwarded message is going to be sent to a person named Jeff Smith. The message body 102 of the original message 90 is contained within message body 132 of the forwarded message. An indicator or separator line 134 indicates where the
message body 102 of the original message 90 begins.

30 **[0046]** "AR_June.doc" is missing from the message to be forwarded. The user of the mobile communication device recognizes this because that attachment is not shown in region 138 of the device's display. Along with the attachment not being shown in the region 138, it will be understood that there are a number of additional ways in which the user could be

- 13 -

made aware that "AR_June.doc" will not be forwarded. For example, a dialog window could appear to warn the user.

[0047] The attachment does not go with the forwarded message because the messaging application has determined that a MIME attribute for the attachment indicates that content forwarding is not allowed with respect to that attachment. In an example embodiment, the attachment is not to be included with the forwarded message if its MIME attribute is "Content-Forwarding: denied", and the attachment is permitted to be included with the forwarded message if its MIME attribute is "Content-Forwarding: allowed". Parts of a message having the MIME attribute "Content-Forwarding: denied" have a higher level of security than those parts of the message having the MIME attribute "Content-Forwarding: allowed". With respect to the example message from Accounting, the "AR_June.doc" part of the message has a higher level of security than the message text and "Request_Form.doc" message parts.

[0048] Forwarding prevention of one or more message parts (such as the "AR_June.doc" attachment) may reduce security concerns in various situations. As an example, security concerns may be reduced when the original message is in a secure format and the derived message is sent out in a format that is not secure.

[0049] Still with reference to the example message from accounting, Figure 6 is a screen shot 118 illustrating another example of a forwarded message composition derived from the original message 90. In this example, content forwarding is applied to a portion of the message body of the e-mail from accounting. In particular, the name and contact information of the original message are missing from the forwarded message composition because this portion was marked with the MIME attribute "Content Forwarding: denied". Also, in the illustrated example, the user of the device 10 is presented with an explanation embedded in the message notifying the user that the protected portion of the message body has not been included in the forwarded message composition. The user could also be made aware in alternative ways that a security

- 14 -

precaution has been offended and that one or more protected portions of the message were not included in the forwarded message composition. For example, there could simply be a beep that sounds at some point during the message composition process, or a dialog box could pop up to
5 notify the user that one or more portions of the message were not included in the forwarded message composition.

[0050] Although the examples illustrated in Figures 5 and 6 are forwarded message composition examples, it will be understood that, for consistency, it would be desirable to have the messaging application
10 behave in the same manner with respect to a reply-to message composition. Although many messaging applications are configured by default to not have the original attachments included in a reply-to message composition, it could be that (like in the Figure 6 example) the message text itself is to be protected.

15 **[0051]** It will be understood that action prevention in relation to higher security level parts is not limited to those actions that involve content forwarding off of the mobile communication device or other message processing machine. For example, the action prevention in relation to a higher security level part could be preventing the display of
20 the higher level security part on a display in those situations when the message part does not even need to be sent to a server for decoding. This might be done if, for example, there were concerns about not being able to view the higher level security part in a font believed to make displayed text more tempest resistant. As another example, the e-mail security
25 module 57 could be configured to force the display of any higher level security part in a font believed to make displayed text more tempest resistant. For instance, a user of the device 10 might have preconfigured the messaging application 56 to have the text in the message body 102 (Figure 3) displayed in a font of his liking, but that font might not be the
30 font believed to make displayed text more tempest resistant. Consequently, the module 57 could prevent the action of having the text in the message body 102 displayed in the default font, the text instead being displayed in a font perceived to be more tempest resistant.

- 15 -

[0052] The information provided by the MIME attribute need not be as simple as "denied" and "allowed". For example, a more granular system could be used to give finer detail on when to include the particular message part. In a classification system, there could be a number of
5 levels of security. For instance, there could be four levels of security such as classified, confidential, secret and top secret, with top secret as the top level and classified as the bottom level. The messaging application of the user's mobile communication device could then be set up so that certain restrictions only apply above a certain level. For example, a message part
10 having a security level of confidential or lower might be included in a forwarded message, but a message part having a security level of secret or higher might not be included in the forwarded message. In this case the threshold would be between confidential and secret. Of course any number of levels of security could be chosen for a classification system
15 (e.g. three, four, five, etc.), and the levels between which the threshold(s) would be set could vary from one user to another.

[0053] One skilled in the art will appreciate that there might be situations where a server in communication with the user's mobile communication device could have access to the user's private keys. In
20 such cases, the previously described MIME processing could possibly be done at the server rather than at the mobile communication device.

[0054] It will be understood that the needed security information about a message part could be obtained in some other way besides scanning the MIME header of a message part. For instance, in the case
25 where the message part is an e-mail attachment, the information could be contained in the actual contents of the e-mail attachment. The messaging application in this embodiment would not scan the MIME header of the e-mail attachment, but would instead extract the needed information from the e-mail attachment part, for example.

30 **[0055]** The present invention may be embodied in other specific forms without departing from the spirit or essential characteristics thereof. Certain adaptations and modifications of the invention will be obvious to

- 16 -

those skilled in the art. Therefore, the above discussed embodiments are considered to be illustrative and not restrictive, the scope of the invention being indicated by the appended claims rather than the foregoing description, and all changes which come within the meaning and range of
5 equivalency of the claims are therefore intended to be embraced therein.

- 17 -

CLAIMS:

1. A method of handling an electronically transmitted message (74) having at least two parts (102,116) with a higher level security part (116) having a higher level of security than the other part (102), the method
5 comprising:
 - receiving a request to forward said electronically transmitted message (74);
 - composing a forwarded message;
 - including, in said forwarded message, said other part (102);
 - 10 extracting an attribute from said electronically transmitted message (74), said attribute indicating that said higher level security part (116) is not permitted to be forwarded; and
 - including, in said forwarded message, an indication that said higher level security part (116) has not been included.
- 15 2. A method as claimed in claim 1, wherein said message (74) is an email message.
3. A method as claimed in claim 1 or claim 2, wherein said higher level security part (116) is an email attachment.
4. A method as claimed in any of claims 1 through 3 further comprising
20 transmitting said forwarded message.
5. A computer program product having a computer readable medium tangibly embodying computer executable instructions for implementing in a computing device (10) the method of any one of claims 1 to 4.
6. A handheld electronic device (10) having a messaging application (56)
25 permitting a recipient of an electronically transmitted message (74) to take actions in relation to the message (74), said electronically transmitted

- 18 -

message (74) having at least two parts (102, 116) with a higher level security part (116) having a higher level of security than the other part (102), the handheld device (10) comprising:

a display screen (22);

5 a processor (38) in electronic communication with said display screen (22), said processor (38) capable of controlling operation of said display screen (22);

and wherein:

10 at least one computer readable medium storing code and in electronic communication with said processor, the code comprising:

computer executable instructions for receiving a request to forward said electronically transmitted message (74);

computer executable instructions for composing a forwarded message;

15 computer executable instructions for including, in said forwarded message, said other part (102);

20 computer executable instructions for extracting an attribute from said electronically transmitted message (74), said attribute indicating that said higher level security part (116) is not permitted to be forwarded; and

computer executable instructions for including, in said forwarded message, an indication that said higher level security part (116) has not been included.

25 7. A handheld device (10) as claimed in claim 6, wherein a classification system is arranged to determine if forwarding is permitted in relation to each of said at least two parts.

- 19 -

8. A handheld device (10) as claimed in claim 7, wherein said classification system comprises at least three levels of security.

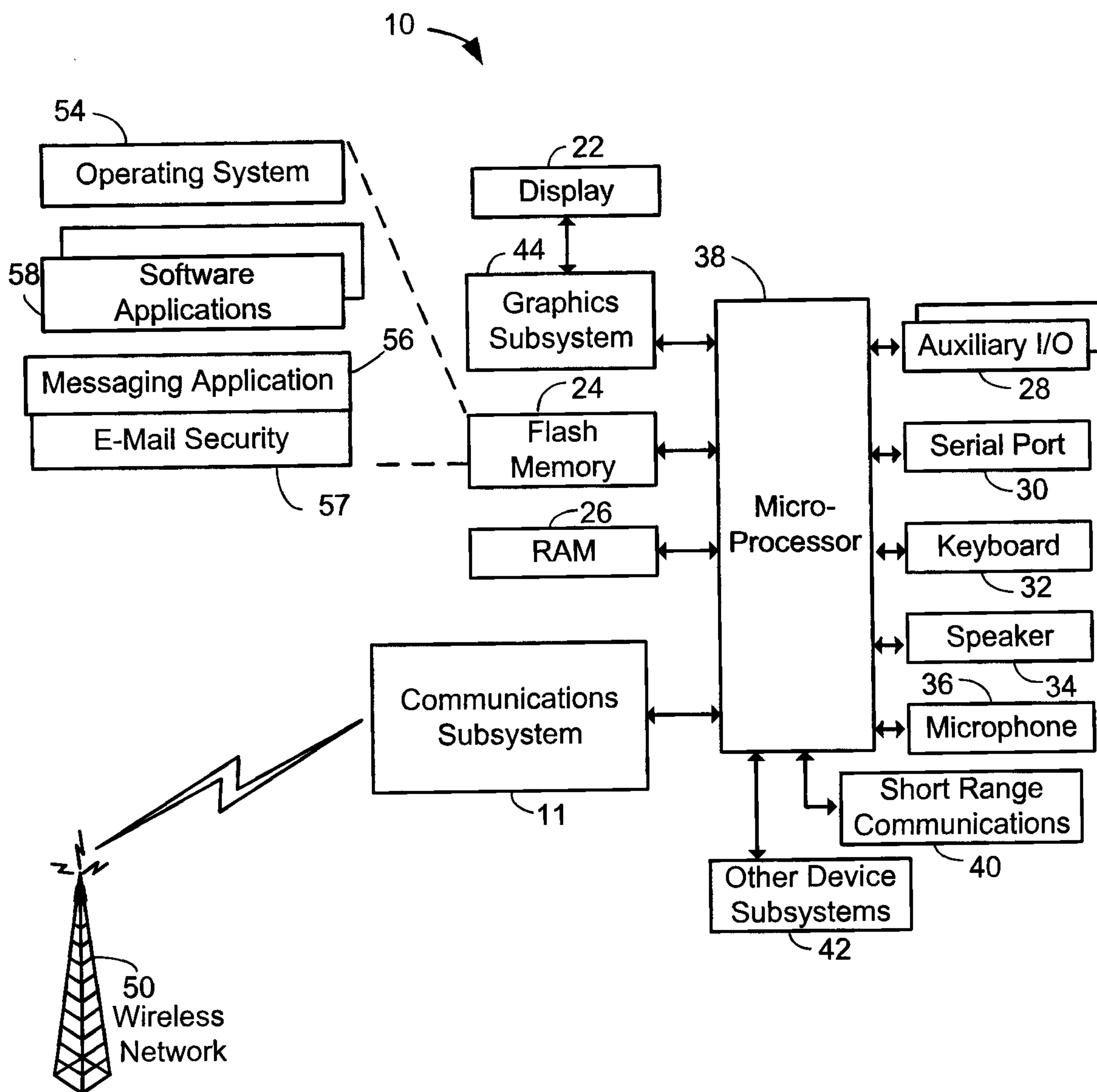
9. A handheld device (10) as claimed in claim 8, wherein one of said levels of security is associated with said higher level security part (116) of the message (74) and a different and lower one of said levels of security is associated with said other part (102) of the message (74).

10. A handheld device (10) as claimed in any one of claims 6 to 9, wherein said higher level security part (116) of the message (74) is an attached word processing document and said other part (102) of the message (74) is message text.

11. A communication system comprising a plurality of handheld electronic devices (10) according to any one of claims 6 to 10.

Ridout & Maybee LLP
Suite 2400
One Queen Street East
Toronto, Canada M5C 3B1
Patent Agents of the Applicant

1/4

Fig. 1

2/4

70	78	82	86	
	☐	Daily News	Your Daily News Update	74
	☐	ABC Group	Reminder	74
	88	John Doe	Hello There	74
	88	Accounting	AR Reports	90
	88	Sports Update	Baseball Scores	74
	☐	Sports Update	Football Scores	

Fig. 2

94

98

102

104

From: Accounting
Subject: AR Reports

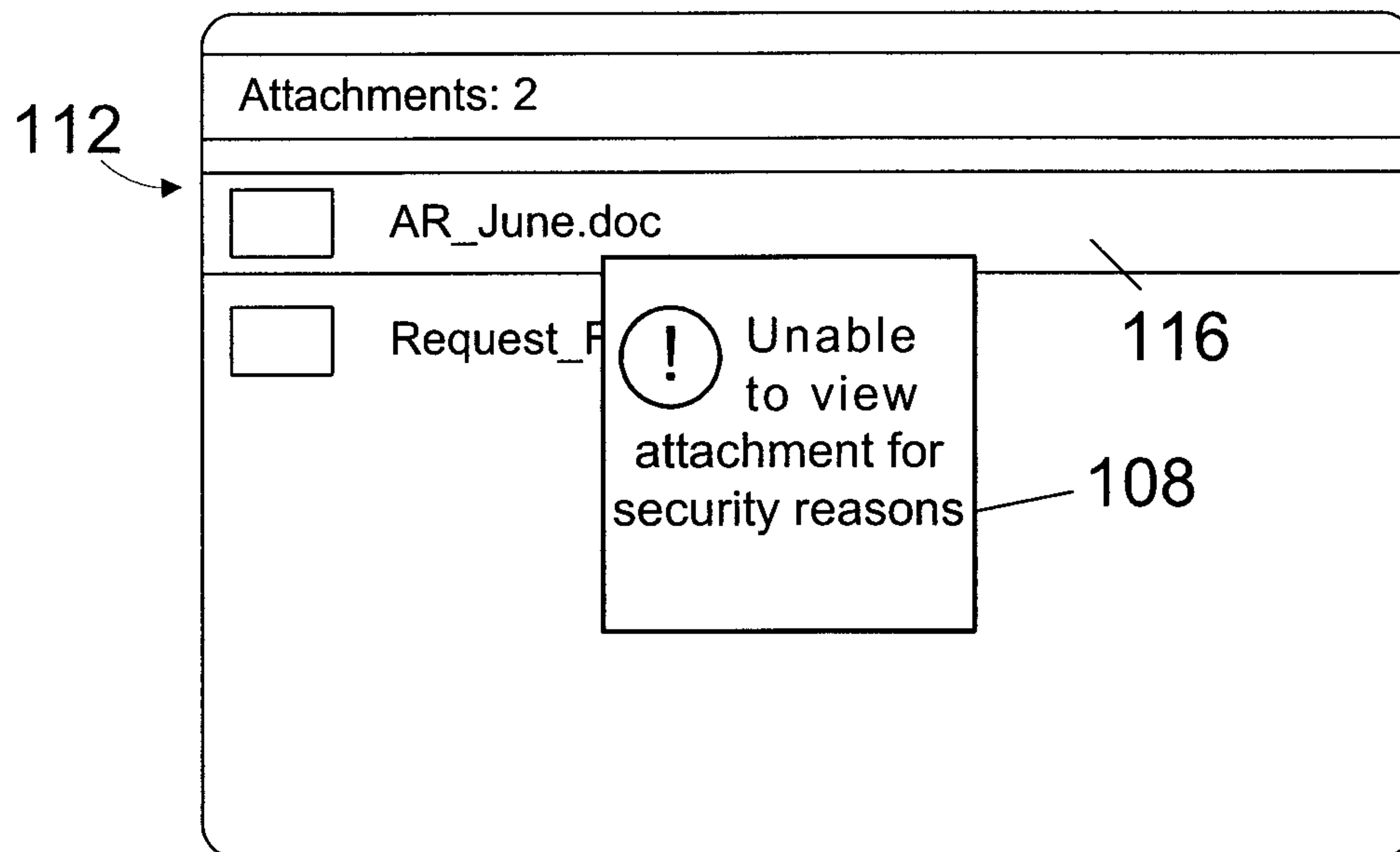
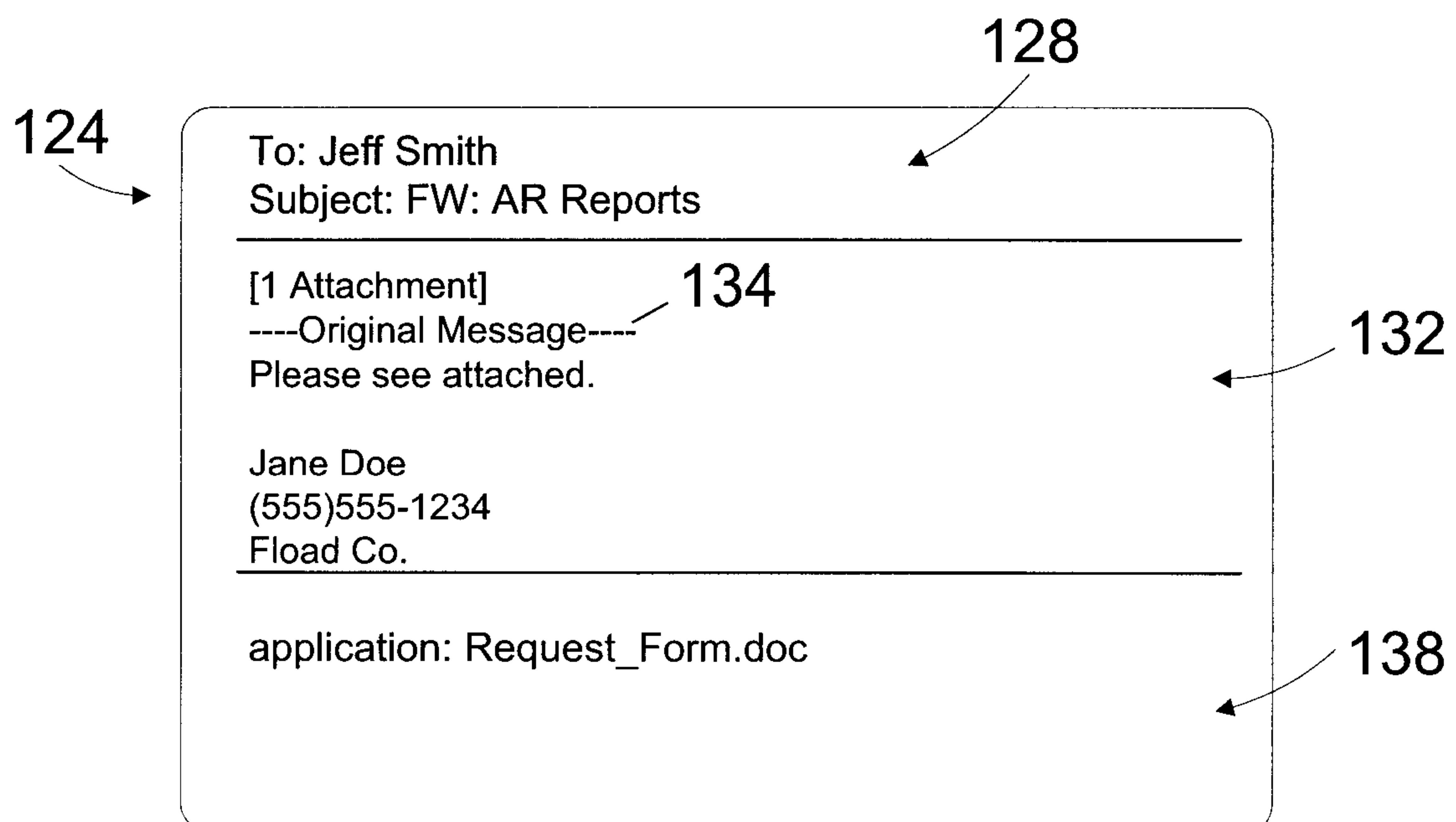
[2 Attachments]
Please see attached.

Jane Doe
(555)555-1234
Fload Co.

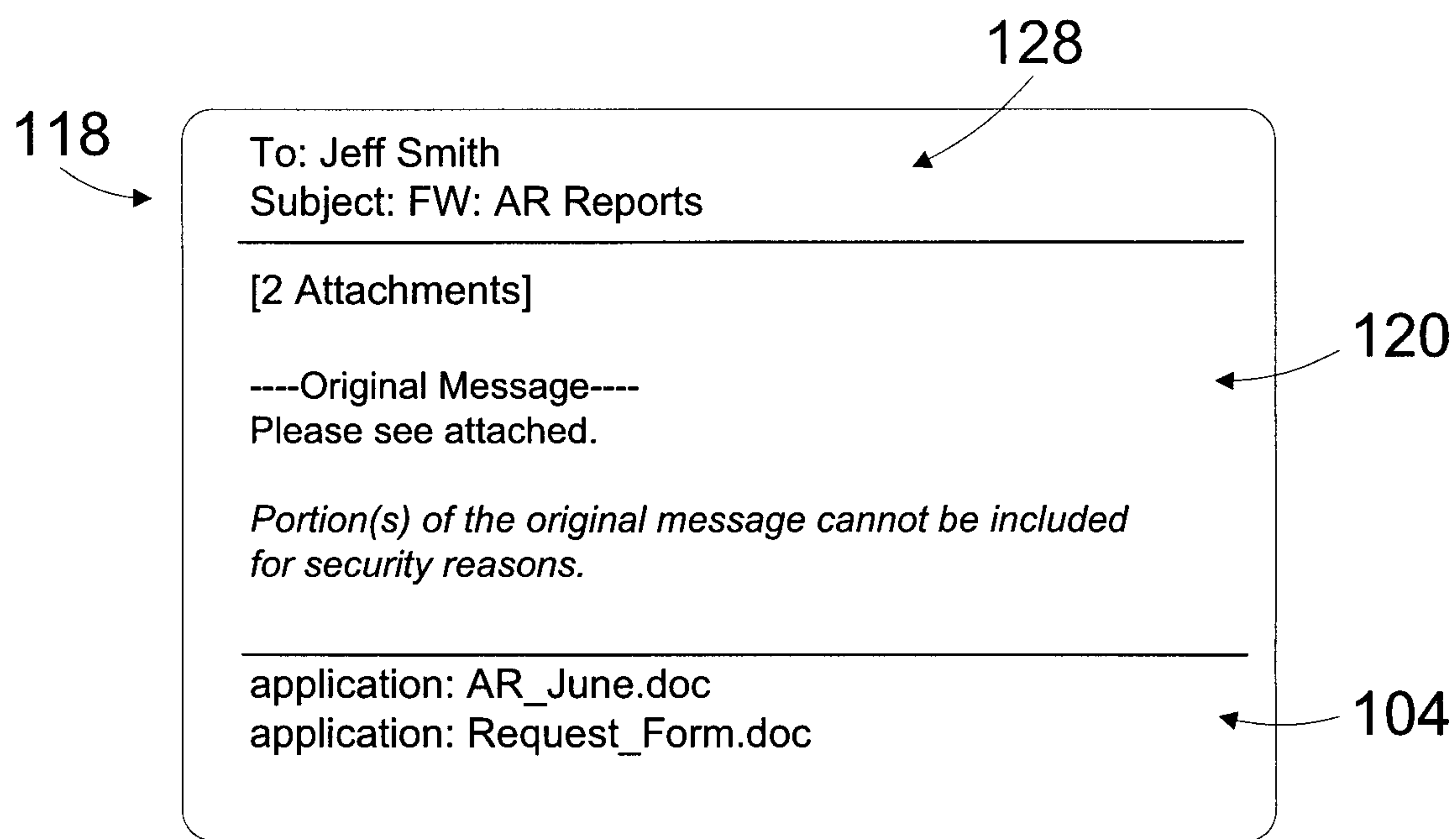
application: AR_June.doc
application: Request_Form.doc

Fig. 3

3/4

Fig. 4Fig. 5

4/4

Fig. 6

Attachments: 2



AR_June.doc



Request_F



Unable
to view
attachment for
security reasons

116

108

112