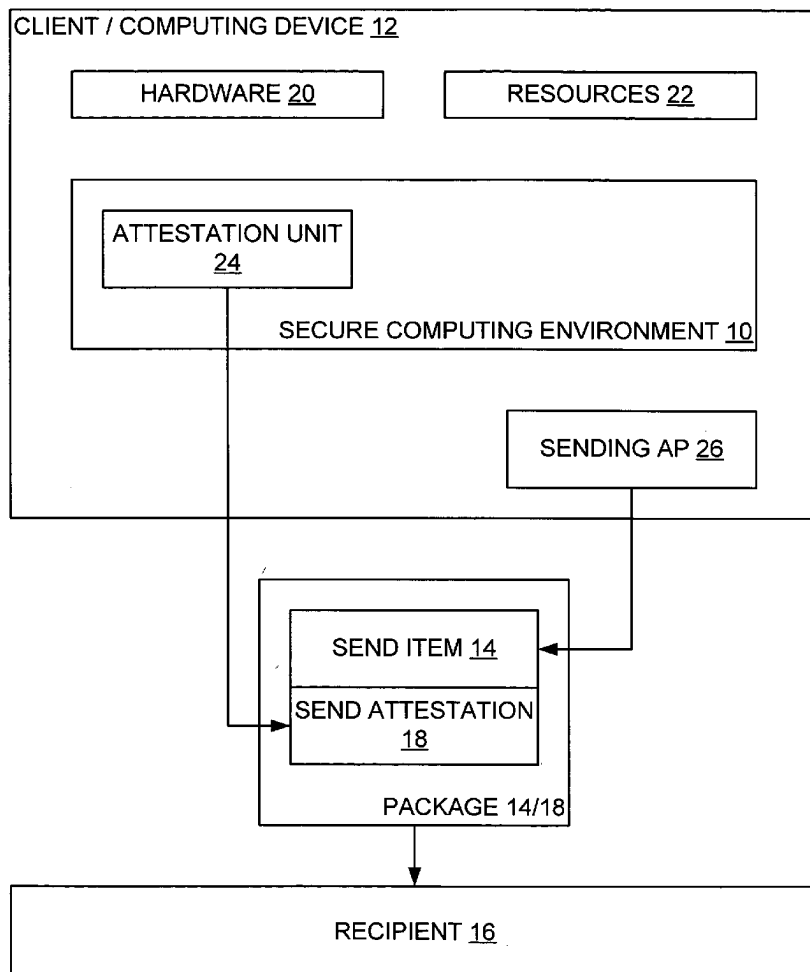


(19) **United States**(12) **Patent Application Publication** (10) **Pub. No.: US 2005/0278253 A1**
(43) **Pub. Date: Dec. 15, 2005**(54) **VERIFYING HUMAN INTERACTION TO A
COMPUTER ENTITY BY WAY OF A
TRUSTED COMPONENT ON A COMPUTING
DEVICE OR THE LIKE****Publication Classification**(51) **Int. Cl.⁷** **G06F 17/60**(52) **U.S. Cl.** **705/50**(75) **Inventors:** **Christopher A. Meek**, Kirkland, WA
(US); **David Earl Heckerman**,
Bellevue, WA (US); **Josh D. Benaloh**,
Redmond, WA (US); **Marcus Peinado**,
Bellevue, WA (US); **Joshua Theodore**
Goodman, Redmond, WA (US)(57) **ABSTRACT**

A method describes user interaction in combination with sending a send item from an application of a computing device to a recipient. The computing device has an attestation unit thereon for attesting to trustworthiness. The application facilitates a user in constructing the send item, and pre-determined indicia are monitored that can be employed to detect that the user is in fact expending effort to construct the send item. The attestation unit authenticates the application to impart trust thereto, and upon the user commanding the application to send, a send attestation is constructed to accompany the send item. The send attestation is based on the monitored indicia and the authentication of the application and thereby describes the user interaction. The constructed send attestation is packaged with the constructed send item and the package is sent to the recipient.

Correspondence Address:

WOODCOCK WASHBURN LLP
ONE LIBERTY PLACE - 46TH FLOOR
PHILADELPHIA, PA 19103 (US)(73) **Assignee:** **Microsoft Corporation**, Redmond, WA(21) **Appl. No.:** **10/868,116**(22) **Filed:** **Jun. 15, 2004**

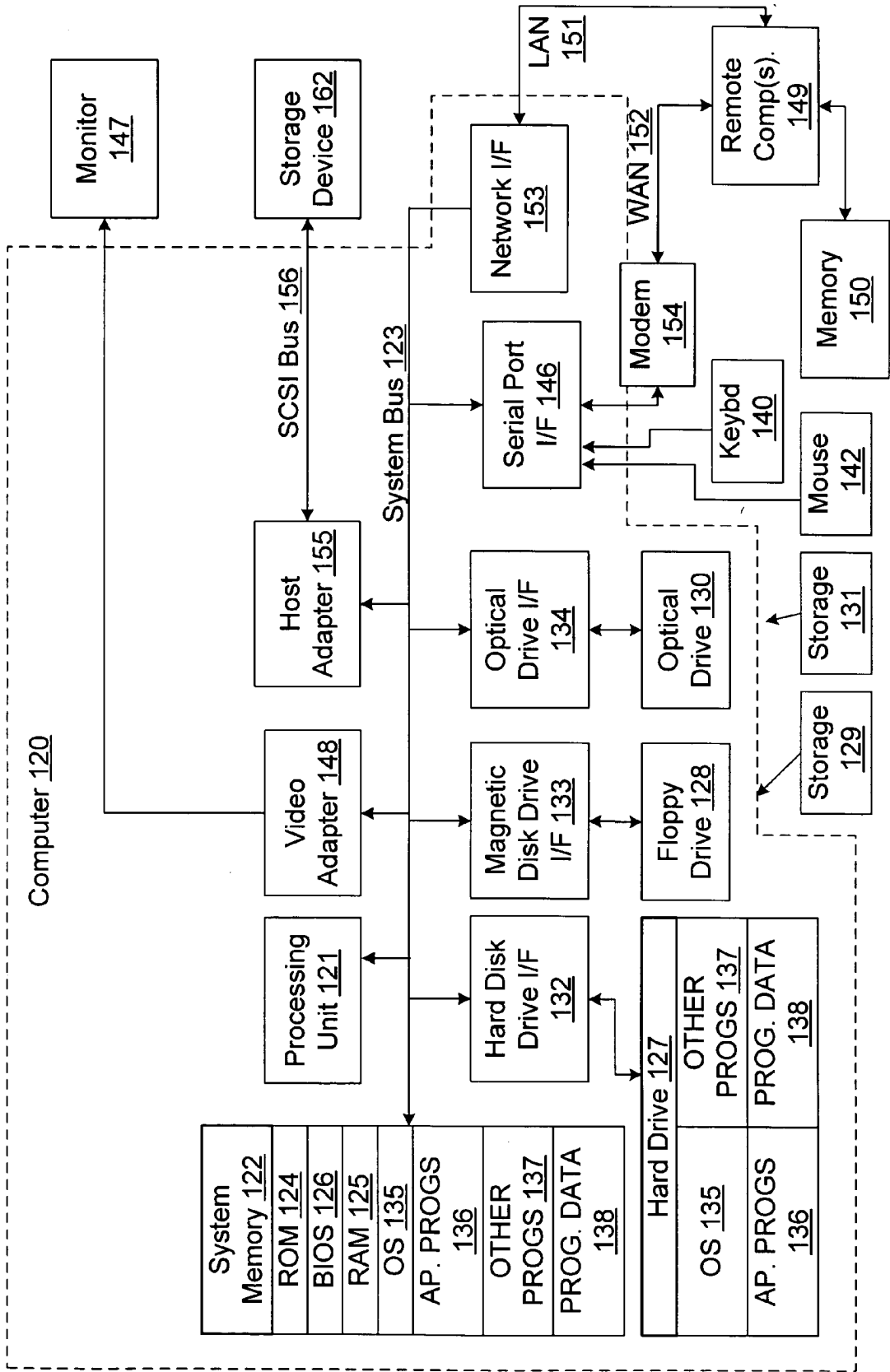


Fig. 1

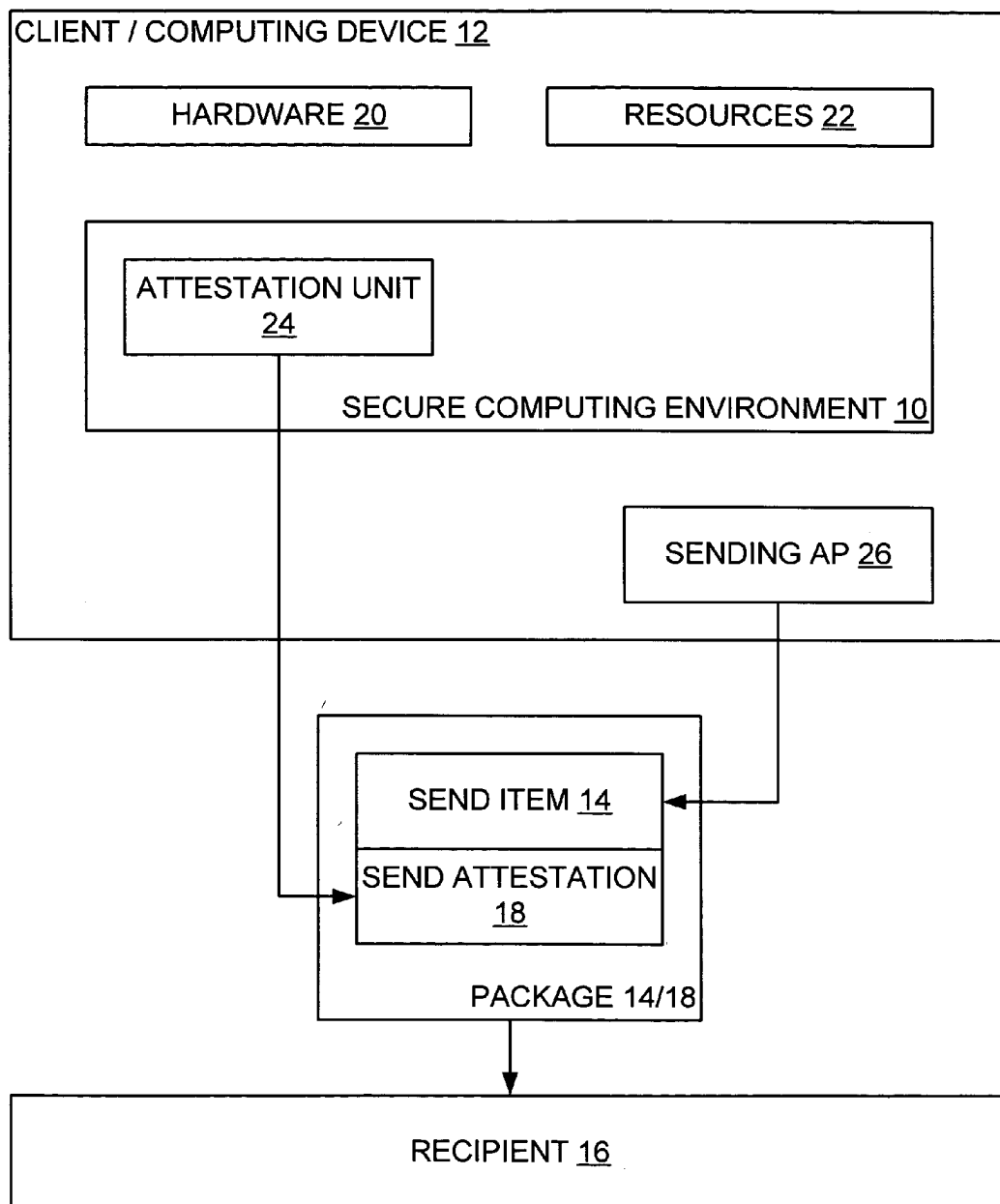
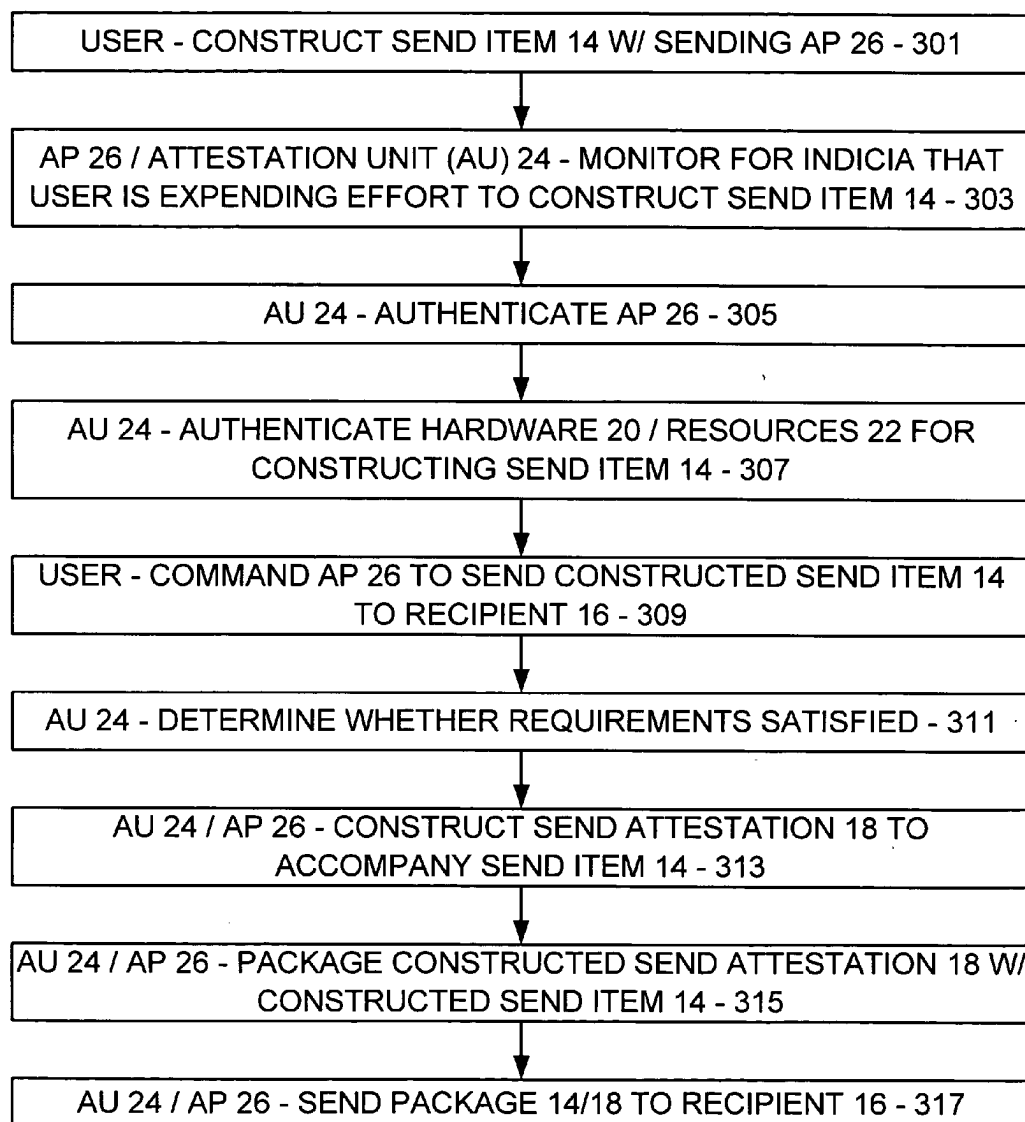


Fig. 2

**FIG. 3**

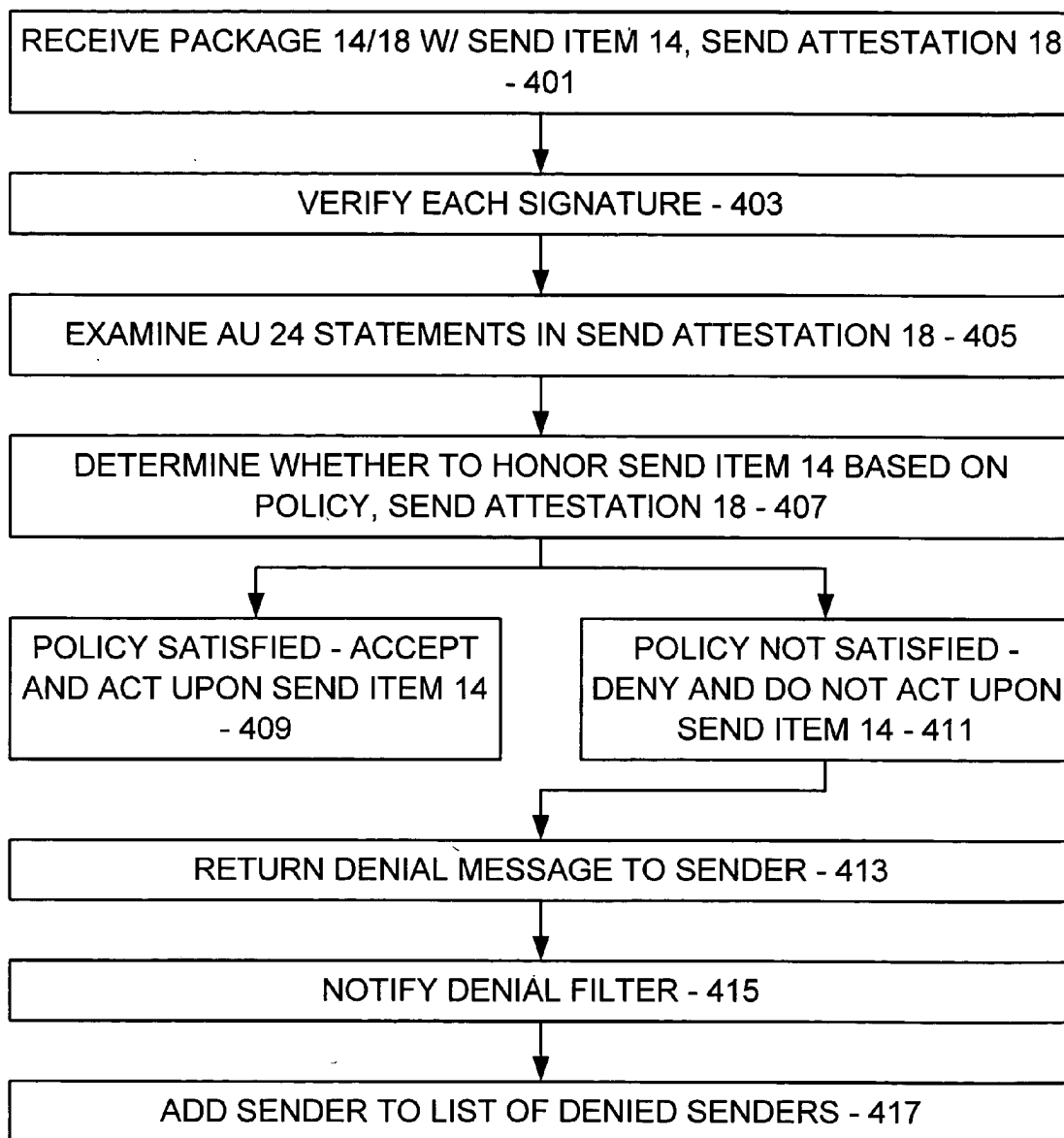


FIG. 4

**VERIFYING HUMAN INTERACTION TO A
COMPUTER ENTITY BY WAY OF A TRUSTED
COMPONENT ON A COMPUTING DEVICE OR
THE LIKE**

TECHNICAL FIELD

[0001] The present invention relates to an architecture and method for verifying to a computer entity that a computer request made in connection with a computing device originated from a human and not from a computer application or the like. More particularly, the present invention relates to such an architecture and method whereby the verification is performed by way of a trusted component operating on the computing device.

BACKGROUND OF THE INVENTION

[0002] Human Interactive Proofs exist to demonstrate to a computer entity that a request to the entity from a computing device originates from a human at the computing device, and not merely from an application running on the computing device. Thus, such a Human Interactive Proof may be employed for example by a network site to confirm that a request for a site ID is from a human attempting to obtain a single site ID for a presumably legitimate purpose, and that such request is not from a computer application attempting to obtain multiple site IDs for a presumably illegitimate or at least unwelcome purpose. As may be appreciated, in the latter case such multiple site IDs may be employed for example by a nefarious entity wishing to hide behind such multiple site IDs in order to avoid truthfully identifying oneself.

[0003] Such a Human Interactive Proof also may be employed for example by a message recipient to confirm that a sender of a message is a human attempting to send a personal message to the recipient for a presumably welcome purpose, and that such message is not from a computer application attempting to send multiple non-personal bulk messages for a presumably unwelcome purpose. As may be appreciated, in the latter case such multiple bulk messages may for example take the form of advertising or 'spam' from a nefarious entity having no personal relationship to the recipient.

[0004] A Human Interactive Proof may further be employed for example by an on-line advertiser that pays a referral fee to an on-line intermediary each time a link provided by the intermediary is selected by a user. Here, the Proof confirms that a message is from a human selecting user human wishing to access the advertiser by way of the link, and that such message is not from a computer application attempting to send multiple non-personal bulk messages to the advertiser from the intermediary or an agent thereof. As may be appreciated, in the latter case such multiple bulk messages may for example be sent merely to generate referral fees even though no end user is involved, and is sometimes referred to as 'fraudulent click-through'. As may be further appreciated, such fraudulent click-through can occur in advertising settings and in other settings where an intermediary has an incentive to generate such messages.

[0005] More generally, it is to be appreciated that Human Interactive Proofs are employed to prevent unwanted bulk-sent messages, prevention of fraudulent click-through in an

advertising setting or the like, prevention of predatory sniping on online auction sites, human proof for online purchases, human proof for account setup, and the like. Such Human Interactive Proofs, then, may be employed in any situation where a recipient of a request or message (hereinafter, 'send item') wishes to ensure that the send item originated from a human at a computing device performing human-type actions, and not merely the computing device performing programmed actions.

[0006] Each such Human Interactive Proof is essentially designed to require that a human sending the aforementioned send item expend some sort of active effort, where the effort is of the nature of an action that a computing device likely cannot perform. In one popular version of a Human Interactive Proof, for example, the prospective recipient sends to the prospective sender a 'challenge' comprising a picture of an article that may be described easily with one word, such as a dog, a ball, a pencil, etc., and the sender must send the one word with the send item. Presumably, if the sender is human, such sender can easily recognize the pictured article in the challenge and provide the word. Also presumably, if the sender is not a human but is a computing device, such sender cannot easily recognize the pictured article and provide the word. In another popular version of a Human Interactive Proof, the prospective recipient sends to the prospective sender a challenge comprising a picture of a word that is not expected to be easily recognizable based on optical character recognition protocols that maybe performed by a computing device, but that should be easily recognizable to a human, and the sender again must send the word with the send item.

[0007] At any rate, failure to provide the word with the send item may for example cause the prospective recipient to ignore the message based on the presumption that the sender is not a human sending a welcome send item. Since the effort to recognize the picture or word and provide the one word can not easily be performed by a computing device, the Human Interactive Proof for the most part establishes that the sender of the request or message is a human.

[0008] Moreover, even if the effort to recognize can somehow be performed by a computing device, or if a nefarious entity can employ human laborers to perform the recognitions, the effort imposes a cost on the computing device or laborer employer as sender, either in terms of monetary value, capacity, time, or the like. For example, a computing device sending out an email message to one million recipients may do so with relative ease based on current technologies if no Human Interactive Proof is required for each of the one million messages. However, and significantly, the same computing device sending out an email message to one million recipients must expend tremendous effort if a unique Human Interactive Proof is required for each of the one million messages. As may be appreciated, then, requiring a computing device or human laborer to perform a Human Interactive Proof for each of many send items can quickly become a severe hindrance, especially in the case where the computing device or laborer employer is attempting to send out hundreds, thousands, or even millions of such send items.

[0009] To summarize, then, Human Interactive Proofs prevent unwanted send items, such as those that may be sent

out in bulk by a computing device, because the Human Interactive Proofs require the computing device to perform an action that the computing device cannot in fact perform, or else require the computing device or a human laborer to perform the action on a per send item basis and thus expend tremendous effort. Human Interactive Proofs to date suffer, however, in that such Proofs require the human to expend an active effort in order to satisfy such Proofs, and do not account for passive efforts that the human may expend in the natural course of sending an item. Put another way, current Human Interactive Proofs do not recognize that a human in sending an item expends passive or natural efforts that a computer cannot likewise expend, such as for example typing on a keyboard, moving a cursor by way of a mouse device, etc., and that by detecting expending of such passive efforts a Human Interactive Proof need not in fact require the human to expend an active or specific effort in the manner of 'jumping through a hoop'.

[0010] A need exists, then, for a Human Interactive Proof (HIP) that requires essentially no active effort be expended by a human, but that the human only expend natural efforts that are detected. In particular, a need exists for an architecture and method that implements such a Human Interactive Proof, and that verifies such detected natural effort to the recipient in a trusted manner so that the recipient can be assured that the detected natural efforts did in fact occur and were not simply contrived by a nefarious entity attempting to trick the recipient. Further, a need exists for such an architecture and method whereby a trusted component on the computing device of the sender performs such verification.

SUMMARY OF THE INVENTION

[0011] The aforementioned needs are satisfied at least in part by the present invention in which a method is provided to describe user interaction in combination with sending a send item from an application of a computing device to a recipient. The computing device has an attestation unit thereon for attesting to trustworthiness. In the method, the application on the computing device facilitates a user in constructing the send item, and one of the application and the attestation unit monitors for pre-determined indicia that can be employed to detect that the user is in fact expending effort to construct the send item.

[0012] The attestation unit authenticates the application to impart trust thereto, and one of the application and the attestation unit, upon the user commanding the application to send the constructed send item to the recipient, constructs a send attestation to accompany the send item. The send attestation is based on the monitored indicia and the authentication of the application and thereby describes the user interaction. One of the attestation unit and the application packages the constructed send attestation with the constructed send item, and one of the attestation unit and the application sends the packaged send item and send attestation to the recipient.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] The foregoing summary, as well as the following detailed description of the embodiments of the present invention, will be better understood when read in conjunction with the appended drawings. For the purpose of illus-

trating the invention, there are shown in the drawings embodiments which are presently preferred. As should be understood, however, the invention is not limited to the precise arrangements and instrumentalities shown. In the drawings:

[0014] FIG. 1 is a block diagram representing a general purpose computer system in which aspects of the present invention and/or portions thereof may be incorporated;

[0015] FIG. 2 is a block diagram showing a computing device with a sending application and an attestation unit sending a send item and a send attestation to a recipient in accordance with one embodiment of the present invention; and

[0016] FIGS. 3 and 4 are flow diagrams showing key steps performed at the computing device (FIG. 3) and recipient (FIG. 4) of FIG. 2 in accordance with one embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0017] Computer Environment

[0018] FIG. 1 and the following discussion are intended to provide a brief general description of a suitable computing environment in which the present invention and/or portions thereof may be implemented. Although not required, the invention is described in the general context of computer-executable instructions, such as program modules, being executed by a computer, such as a client workstation or a server. Generally, program modules include routines, programs, objects, components, data structures and the like that perform particular tasks or implement particular abstract data types. Moreover, it should be appreciated that the invention and/or portions thereof may be practiced with other computer system configurations, including hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, mini-computers, mainframe computers and the like. The invention may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

[0019] As shown in FIG. 1, an exemplary general purpose computing system includes a conventional personal computer 120 or the like, including a processing unit 121, a system memory 122, and a system bus 123 that couples various system components including the system memory to the processing unit 121. The system bus 123 may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures. The system memory includes read-only memory (ROM) 124 and random access memory (RAM) 125. A basic input/output system 126 (BIOS), containing the basic routines that help to transfer information between elements within the personal computer 120, such as during start-up, is stored in ROM 124.

[0020] The personal computer 120 may further include a hard disk drive 127 for reading from and writing to a hard disk (not shown), a magnetic disk drive 128 for reading from or writing to a removable magnetic disk 129, and an optical

disk drive **130** for reading from or writing to a removable optical disk **131** such as a CD-ROM or other optical media. The hard disk drive **127**, magnetic disk drive **128**, and optical disk drive **130** are connected to the system bus **123** by a hard disk drive interface **132**, a magnetic disk drive interface **133**, and an optical drive interface **134**, respectively. The drives and their associated computer-readable media provide non-volatile storage of computer readable instructions, data structures, program modules and other data for the personal computer **120**.

[0021] Although the exemplary environment described herein employs a hard disk, a removable magnetic disk **129**, and a removable optical disk **131**, it should be appreciated that other types of computer readable media which can store data that is accessible by a computer may also be used in the exemplary operating environment. Such other types of media include a magnetic cassette, a flash memory card, a digital video disk, a Bernoulli cartridge, a random access memory (RAM), a read-only memory (ROM), and the like.

[0022] A number of program modules may be stored on the hard disk, magnetic disk **129**, optical disk **131**, ROM **124** or RAM **125**, including an operating system **135**, one or more application programs **136**, other program modules **137** and program data **138**. A user may enter commands and information into the personal computer **120** through input devices such as a keyboard **140** and pointing device **142**. Other input devices (not shown) may include a microphone, joystick, game pad, satellite disk, scanner, or the like. These and other input devices are often connected to the processing unit **121** through a serial port interface **146** that is coupled to the system bus, but may be connected by other interfaces, such as a parallel port, game port, or universal serial bus (USB). A monitor **147** or other type of display device is also connected to the system bus **123** via an interface, such as a video adapter **148**. In addition to the monitor **147**, a personal computer typically includes other peripheral output devices (not shown), such as speakers and printers. The exemplary system of **FIG. 1** also includes a host adapter **155**, a Small Computer System Interface (SCSI) bus **156**, and an external storage device **162** connected to the SCSI bus **156**.

[0023] The personal computer **120** may operate in a networked environment using logical connections to one or more remote computers, such as a remote computer **149**. The remote computer **149** may be another personal computer, a server, a router, a network PC, a peer device or other common network node, and typically includes many or all of the elements described above relative to the personal computer **120**, although only a memory storage device **150** has been illustrated in **FIG. 1**. The logical connections depicted in **FIG. 1** include a local area network (LAN) **151** and a wide area network (WAN) **152**. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets, and the Internet.

[0024] When used in a LAN networking environment, the personal computer **120** is connected to the LAN **151** through a network interface or adapter **153**. When used in a WAN networking environment, the personal computer **120** typically includes a modem **154** or other means for establishing communications over the wide area network **152**, such as the Internet. The modem **154**, which may be internal or external, is connected to the system bus **123** via the serial port interface **146**. In a networked environment, program mod-

ules depicted relative to the personal computer **120**, or portions thereof, may be stored in the remote memory storage device. It will be appreciated that the network connections shown are exemplary and other means of establishing a communications link between the computers may be used.

[0025] Verifying Human Interaction By Detecting Passive Effort

[0026] In the present invention, a method and architecture are provided to implement a Human Interactive Proof that verifies that a human is involved in a computing transaction, whereby the human is sending an item to a recipient. In the Proof, and in general, the sent item is accompanied by a send attestation stating to the effect that a sufficient human effort was in fact detected in connection with the sent item, and correspondingly that the computer did not simply send the item based on a program or application that does not require any significant human effort on a per send item basis. The sufficient human effort detected may for example include a keystroke, a mouse click, a minimum number of keystrokes or mouse clicks, a minimum composition time, a selection of a maximum number of recipients, a maximum number of send items delivered per unit time, etc. In the invention, the human interaction is detected passively so that the human need not exert any active effort in connection with the send attestation. Thus, the human interaction is detected based on activities that a human would normally undertake in the course of constructing and sending a send item to a recipient thereof.

[0027] To impart trust to the send attestation, and turning now to **FIG. 2**, such send attestation **18** is composed by or on behalf of a secure computing environment **10** operating on the computing device **12** of the sender of the send item **14**, where the secure computing environment **10** is to be trusted by the recipient **16**. As maybe appreciated, the send item **14** is constructed by or in connection with the computing device **12**, such as for example with the aid of a sending application **26** running on the computing device **12**, and the send attestation **18** is also composed on the computing device **12**. The secure computing environment **10** is configured to provide the send attestation **18** to the recipient **16** on a trusted basis to confirm that the sufficient human effort was detected in connection with the construction of the corresponding send item **14**, again on a passive basis and without requiring any active involvement from the human. In various embodiments, the send item **14** includes the send attestation **18** as an attached object or the like, or the send attestation **18** is separate from but linked to the send item **14**, perhaps by way of a pointer or other reference.

[0028] The computing device **12** of the sender may be any appropriate computing device without departing from the spirit and scope of the present invention. For example, the computing device may be a personal computer, a portable communications device, a wireless communications device, etc. Such computing device **12** is appropriately coupled to the recipient **16** by way of an appropriate communications link. Such link may be a direct connection or may be a network connection such as an intra- or inter-network connection employing appropriate communications protocols.

[0029] The recipient **16** is typically an application running on a server, computer, or other computing device at a location remote from or local to the computing device **12**.

Such recipient **16** may provide a service the sender at the computing device **12** based on a request therefrom, which in this case is in the form of the send item **14**. Thus, the send item **14** may be a request for a piece of content, a request for a user ID, a request for a network resource, etc. The recipient **16** may alternatively receive a message for a user thereat, which in this case is again in the form of the send item **14**. Thus, the send item **14** may also be for example a network message in the form of a mail item. It should be appreciated, then, that the send item **14** is appropriately directed to a corresponding recipient **16**. Such send item **14** and corresponding recipient **16** may therefore be any appropriate send item **14** and recipient **16** without departing from the spirit and scope of the present invention.

[0030] The secure computing environment **10** operating on the computing device **12** of the sender of the send item **14** is as was set forth above a secure computing environment to be trusted by the recipient **16**. Thus, the secure computing environment **10** should be able to demonstrate such trust to the recipient **16**, such as for example by way of being able to proffer a key, digital signature, digital certificate, or the like. Typically, such a digital certificate includes a chain of certificates leading back to a root trust authority, and the recipient **16** accepts the digital certificate and grants trust based thereon if the recipient **16** recognizes and honors the root trust authority of such certificate.

[0031] As may be appreciated, the secure computing environment **10** operating on the computing device **12** of the sender should be free of control by other entities operating on the computing device **12** thereof or of control by other entities, either from other computing devices or of human form. Thus, the secure computing environment **10** should not be able to be forced to issue a send attestation **18** when such send attestation **18** is not warranted, such as for example may be the case should a nefarious entity wish to issue a send item **14** without appropriate human interaction.

[0032] Such secure computing environment **10** may be any appropriate secure computing environment without departing from the spirit and scope of the present invention, subject of course to the constraints set forth herein. For example, the secure computing environment **10** may be a trusted portion of an operating system on the computing device **12**, where the trusted portion of such operating system is free of undue external influence. The secure computing environment **10** may either itself detect sufficient human effort in connection with a send item **14** or impart trust in some application running thereon and perhaps related hardware to so detect, and likewise may either itself construct a send attestation **18** for the send item **14** as appropriate or impart trust in some application running thereon to so construct. In one embodiment of the present invention, the secure computing environment **10** in fact includes an attestation unit **24** as an application running thereon and/or hardware running therein to detect the aforementioned sufficient human effort and to construct the aforementioned send attestation **18**.

[0033] The attestation unit **24** may be any appropriate hardware and/or software without departing from the spirit and scope of the present invention. For example, the attestation unit **24** may be established as trusted software running in a trusted area of the secure computing environment **10**, or may be a piece of hardware on the computing device **12** that

is designed to perform the attestation functions set forth herein. In either case, such attestation unit **24** is protected from being monitored or influenced by any other software or hardware operating on the computing device, and especially is protected against attacks such as may be employed by a nefarious entity that would attempt to subvert the function of the attestation unit **24**. The attestation unit **24**, then, should be designed to be tamper resistant, and should be capable of digitally signing, verifying a signature, encrypting, decrypting, and the like. Such an attestation unit **24** at a minimum should be apparent to the relevant public and therefore need not be set forth herein in any detail.

[0034] Note that the secure computing environment **10** and/or attestation unit **24** thereof in detecting whether sufficient human effort has been expended likely must accept inputs that derive from hardware **20** on the computing device **12** that a human would employ in the course of constructing a send item **14**. For example, such hardware **20** may include a touch screen, a keyboard, a cursor control device such as a mouse, and the like. In addition, the secure computing environment **10**/attestation unit **24** (hereinafter, attestation unit **24**) may refer to other resources **22** of the computing device **12** such as a clock, memory, a controller, and the like. Each such piece of hardware **20** and each such resource **22**, then, may become an avenue by which a nefarious entity might attempt to improperly subvert detection of expending of sufficient human effort in connection with a send item **14**. Accordingly, and in one embodiment of the present invention, each such piece of hardware **20** and each such resource **22** is constructed to be trusted by the attestation unit **24**, and also to be able to demonstrate such trust to the attestation unit **24**, such as for example by way of being able to proffer a key, digital signature, digital certificate, or the like. Again, such a digital certificate typically includes a chain of certificates leading back to a root trust authority, and the secure computing environment **10** accepts the digital certificate and grants trust based thereon if such attestation unit **24** recognizes and honors the root trust authority of such certificate.

[0035] The send attestation **18** itself may take any appropriate form without departing from the spirit and scope of the present invention. For example, the send attestation **18** may be constructed as a digital document based on some form of extensible Markup Language (XML) and may be digitally signed based on a private key and verifiable according to a corresponding public key available from the aforementioned digital certificate of the secure computing environment **10**, or a digital certificate of the attestation unit **24**. Thus, such send attestation **18** may include such digital certificate, and also may contain some sort of positive statement attesting to the fact that sufficient human effort was detected as being expended in the course of constructing the corresponding send item **14**. In addition, it may be the case that the send attestation **18** includes details relating to such detected expended human effort, such as for example a number of keystrokes, an amount of time employed to construct the send item **14**, a number of recipients **16**, etc., a number of send items **14** sent during a previous pre-defined period, and/or details relating to hardware **20** and/or resources **22** employed. As may be appreciated, with such details the recipient **16** may perform additional filtering in the course of deciding whether to honor the send item **14**.

[0036] To summarize then, in the present invention, the sending user sending a send item 14 to a recipient 16 employs a computing device 12 with hardware 20 including some sort of input device such as a keyboard, a mouse, etc.; resources 22 including memory and the like; an application 26 for constructing the send item 14; and a trusted attestation unit 24 operating in a secure computing environment 10 that cannot be influenced by the user and that can attest to the send item 14. The recipient 16 upon receiving the send item 14 and accompanying send attestation 18 honors the send item 14 only if the send attestation accompanying same is acceptable to such recipient 16. Turning now to FIG. 3, a method employed by and/or in connection with the aforementioned components is shown.

[0037] Preliminarily, it is expected that a user at the computing device 12 constructs the send item 14 by way of the sending application 26 (step 301). Of course, if the send item 14 is a message, the application 26 is a message-sending application such as an electronic mail application, while if the send item 14 is a request, the application 26 is an application capable of composing the request, such as for example a computer browser based on received code from the recipient 16.

[0038] In connection with constructing the send item 14 as at step 301, one of the application 26 and the attestation unit 24 monitors for some pre-determined indicia that can be employed to detect that the user is in fact expending effort to construct the send item 14 (step 303), and that the application 26 is not itself constructing the send item 14 in the manner of an automated process without substantial user involvement. Such indicia may be any indicia without departing from the spirit and scope of the present invention. For example, the application 26 or attestation unit 24 could monitor for substantial keyboard activity and/or mouse activity, a minimum construction time for constructing the send item 14, a maximum number of send items sent per unit time, the lack of a run script by which activity of the application 26 is controlled, etc.

[0039] Significantly, prior to or after the send item 14 has been constructed as at step 301, the attestation unit 24 authenticates the application 26 (step 305) to impart trust thereto. Such authentication of such application 26 by the attestation unit 24 may for example occur when the application 26 is instantiated on the computing device 12, when the application 26 is called upon by the user to construct the send item 14, or when the send item 14 is constructed and is to be sent to the recipient 16. Such authentication of the application 26 by the attestation unit 24 may comprise any appropriate authentication without departing from the spirit and scope of the present invention. For example, such authentication may comprise the application 26 providing the attestation unit 24 with a digital certificate, and perhaps other operational documentation and perhaps information on the environment within which the application 26 is operating. Based on such information, the attestation unit 24 satisfies itself that the application 26 can be trusted to operate correctly, for example by verifying the digital certificate and ensuring that the application 26 is operating within the environment that is expected based on the operational documentation.

[0040] Note that although the attestation unit 24 could perform the monitoring of step 303, it is to be appreciated

that the application 26 is itself more likely to be to perform such monitoring. Notably, doing so is simpler insofar as the application 26 is monitoring itself, and also in that the application 26 and interfaces thereof may not be well known to the attestation unit 24. At any rate, once the attestation unit 24 trusts the application 26 as at step 305, such trust should extend to the ability of the application 26 to monitor itself as at step 303.

[0041] In conjunction with authenticating the application 26 as at step 305 to impart trust thereto, the attestation unit 24 may also authenticate at least some of the hardware 20 and/or resources 22 that are used or expected to be used in constructing the send item 14 (step 307). Again, such authentication of such hardware 20 and/or resources 22 by the attestation unit 24 may for example occur when the application 26 is instantiated on the computing device 12, when the application 26 is called upon by the user to construct the send item 14, or when the send item 14 is constructed and is to be sent to the recipient 16. As before, such authentication may comprise any appropriate authentication without departing from the spirit and scope of the present invention. For example, and again, such authentication may comprise each of several pieces of hardware 20 and/or resources 22 providing the attestation unit 24 with a digital certificate, and perhaps other documentation and environment information, and based on such information, the attestation unit 24 satisfies itself that, for example, the keyboard can be trusted to operate correctly, the memory can be trusted to operate correctly, etc.

[0042] At any rate, presuming the user has in fact constructed the send item as at step 303, such user then commands the application 26 to in fact send the constructed send item 14 to the recipient 16 (step 309). Upon doing so, the attestation unit 24 determines whether all relevant requirements have been satisfied based on the monitored indicia of step 303 and the authentications of steps 305 and 307 (step 311), and if so, the attestation unit 24 and/or the application 26 constructs the send attestation 18 to accompany such send item 14 (step 313). Thereafter, the attestation unit 24 and/or the application 26 package the constructed send attestation 18 with the constructed send item 14 (step 315), and the application 26 and/or the attestation unit 24 in fact send the packaged send item 14 and send attestation 18 to the recipient 16 (step 317).

[0043] The attestation unit 24 may determine whether all relevant requirements have been satisfied as at step 311 in any appropriate manner without departing from the spirit and scope of the present invention. For example, the attestation unit may require that all authentications as at steps 305 and 307 be successful, and also that the monitored indicia of step 303 meet some predetermined requirements. Such requirements for example may be set forth by the attestation unit 24 or by the recipient 16. In the latter case, it may be that the recipient at some prior time delivered such requirements to the attestation unit 24. Note that in performing step 311, the attestation unit may in fact perform some minimal portion of an overall determination or none at all, and leave the remainder of such determination to the recipient 16. In such case, the attestation unit 24 constructs the send attestation 18 as at step 313 to include all information necessary for the recipient 16 to make the remainder of the determination.

[0044] The attestation unit 24 and/or the application 26 may construct the send attestation 18 as at step 313 in any appropriate manner without departing from the spirit and scope of the present invention. For example, in one embodiment of the present invention, the constructed send attestation 18 includes a statement from the attestation unit 24 describing the application 26, and perhaps the hardware 20 and/or resources 22 employed, and also perhaps relevant information relating to such application 26, hardware 20, and/or resources 22 such as for example the environment thereof. As may be appreciated, such relevant information may be employed by the recipient 16 in deciding whether to accept and honor the send attestation 18 and/or in deciding whether to accept and process the send item 14. Note that while the constructed send attestation 18 may also include a statement from the attestation unit 24 to the effect that the aforementioned application 26, hardware 20 and/or resources 22 are indeed trustworthy, such statement is not believed to be absolutely necessary, especially inasmuch as such a statement is implicit in the fact that the attestation unit 24 chose to issue the statement describing the application 26.

[0045] Significantly, the constructed send attestation 18 also includes a statement describing the send item 14, and also relevant information relating to the send item 14. Notably, such statement may be from the attestation unit 24 or the application 26. In the latter case, the statement from the attestation unit 24 describing the application 26 at least implicitly states that the application 26 can be trusted to issue the statement describing the send item 14. Here, the relevant information relating to the send item 14 in the statement from the attestation unit 24 or application 26 likely includes monitored data such as a number of keyboard taps and/or a number of mouse clicks in connection with construction of the send item 14 by the user, a length of time to construct, a number of recipients 16, etc. As may be appreciated, and again, such relevant information may be employed by the recipient 16 in deciding whether to accept and honor the send attestation 18 and/or in deciding whether to accept and process the send item 14. Note again that while the constructed send attestation 18 may also include a statement to the effect that the send item 14 is indeed trustworthy, such statement is not believed to be absolutely necessary, especially inasmuch as such a statement is implicit in the fact that the attestation unit 24 or application 26 chose to issue the statement describing the send item 14.

[0046] The attestation unit 24 and/or the application 26 may package the constructed send attestation 18 with the constructed send item 14 as at step 315 in any appropriate manner without departing from the spirit and scope of the present invention. For example, in one embodiment of the present invention, the send attestation 18 is appended to the send item 14, and the combined send item 14/send attestation 18 is signed based on a key of the attestation unit 24 to form a digital signature which is appended to the combined send item 14/send attestation 18. As is known, such a digital signature may include or reference a chain of certificates that lead back to a root authority which is presumably known to and trusted by the recipient 16.

[0047] The application 26 and/or the attestation unit 24 may send the packaged send item 14 and send attestation 18 to the recipient 16 as at step 317 in any appropriate manner without departing from the spirit and scope of the present invention. For example, in one embodiment of the present

invention, the computing device 12 of the attestation unit 24/application 26 is coupled to the recipient 16 by way of a network such as an intra- or inter-network, in which case the package 14/18 may be sent by way of one or more network packets according to a mutually acceptable network communications protocol.

[0048] Note that although heretofore described in terms of the attestation unit 24 performing various actions, it could be the case that the attestation unit 24 merely attests to and makes statements about the secure computing environment 10, and that the secure computing environment 10 performs some or all of such actions. In such case, the send attestation 18 may include a statement describing and attesting to the secure computing environment 10.

[0049] Turning now to FIG. 4, upon receiving the package 14/18 with the send item 14 and the send attestation 18 (step 401), the recipient 16 verifies each signature included therein (step 403), including any signature based on a key of the attestation unit 24 and appended to the combined send item 14/send attestation 18. Thereafter, the recipient 16 examines the statements from the attestation unit 24 as set forth in the send attestation 18 from the package 14/18 (step 405). In particular, the recipient 16 decides whether to honor the send item based on the statement describing the application 26 as set forth in the send attestation 18 and the statement describing the send item 14 as set forth in the send attestation 18, among other things.

[0050] In one embodiment of the present invention, such statements as set forth in the send attestation 18 are examined as at step 405 in view of a pre-determined policy set forth by or on behalf of the recipient 16. Such pre-determined policy may be any appropriate policy without departing from the spirit and scope of the present invention. For example, such policy may set forth that the described application 26 must be of a particular type or version, or that such described application 26 not be of a particular type or version. Similarly, such policy may specify a particular environment within which the application 26 is operating, an element that is not to be present in such environment, etc.

[0051] Similarly, and with regard to the send item 14 itself, the policy may for example set forth a particular format of such send item 14, a particular encoding, a limit on the contents of such send item, a limit on the number of recipients of the send item 14, a word that should be in the send item, a word that should not be in the send item, and the like. Significantly, and with regard to the send item 14 itself, the policy may further set forth certain parameters that are relevant to the send item 14 and in particular to factors that might be determinative of whether the send item 14 was indeed constructed based on expended human effort. In this regard, and as may be appreciated, the policy may for example set forth a minimum construction time for the send item 14, a minimum number of keyboard taps, a minimum number of mouse clicks, a maximum number of send items 14 sent per unit time, and the like. Presumptively, and as should be appreciated, each aspect of policy set forth for the recipient 16 can be measured as against information obtained from the statements in the send attestation 18.

[0052] After examining the statements in the send attestation 18 based on policy as at step 405, the recipient 16 then determines whether to in fact honor the send item 14 based on whether the policy is in fact satisfied by the send

attestation 18 (step 407). As should be appreciated, if the policy is in fact satisfied by the send attestation 18, the send item 14 is honored, accepted, and acted upon in whatever manner is deemed appropriate (step 409). For example, if the send item 14 is a message for a user associated with the recipient 16, such send item 14/message is delivered to a receiving area for the user or the like. Likewise, if the send item 14 is a request for a service or an object from the recipient 16 or a related entity, such send item 14/request is delivered to a server or the like that can process same and provide the service or object or the like.

[0053] Note that if the policy is not in fact satisfied by the send attestation 18, the send item 14 is denied and is not honored, accepted, and acted upon (step 411). In such a situation, the recipient 16 could return to the sender at the computing device 12 a simple denial message, a detailed message explaining the denial, or the like (step 413). However, and especially in the case where the sender is some sort of nefarious entity, it may be the case that any return message could bring further unwanted requests or other unwanted attention, and in such case such return message is likely inadvisable.

[0054] The recipient 16 could also in a denial situation notify a denial filter of same (step 415). As may be appreciated, such denial filter would then filter out further requests from the sender of the denied request. In addition or in the alternative, the recipient 16 could also in a denial situation add the sender of the denied request to a list of denied senders (step 417). Here, further requests from the sender would not be filtered out but would be treated differently based on being on such list.

CONCLUSION

[0055] The present invention may be practiced with regard to any appropriate sender sending a send item 14 to a recipient, presuming that such sender and recipient 16 are appropriately configured. As should now be appreciated, with the present invention as set forth herein, sending of a send item 14 to a recipient may be performed in a manner so that the send item 14 is accompanied with a send attestation 18 detailing the human effort expended by the sender.

[0056] The programming necessary to effectuate the processes performed in connection with the present invention is relatively straight-forward and should be apparent to the relevant programming public. Accordingly, such programming is not attached hereto. Any particular programming, then, may be employed to effectuate the present invention without departing from the spirit and scope thereof.

[0057] In the foregoing description, it can be seen that the present invention comprises a new and useful architecture and method for implementing a Human Interactive Proof (HIP) that requires essentially no active effort be expended by a human, but that the human only expend natural efforts that are detected. Such detected natural effort is verified to the recipient 16 by a trusted attestation unit 24 in a trusted manner so that the recipient 16 can be assured that the detected natural efforts did in fact occur and were not simply contrived by a nefarious entity attempting to trick the recipient 16.

[0058] It should be appreciated that changes could be made to the embodiments described above without departing

from the inventive concepts thereof. Most significantly, it is to be appreciated that the present invention may be employed not merely to include indicia of human interaction with a send item 14, but to include any indicia relating to a send item 14, be it of human interaction, machine interaction, or otherwise. Thus, it may for example be the case that the present invention is employed to demonstrate to a recipient 16 that a sending application 26 did not send more than a maximum number of send items 14 per unit time, regardless of any human interaction involved. In general it should be understood, therefore, that this invention is not limited to the particular embodiments disclosed, but it is intended to cover modifications within the spirit and scope of the present invention as defined by the appended claims.

1. A method of sending a send item from an application of a computing device to a recipient, the computing device having an attestation unit thereon for attesting to trustworthiness, the method comprising:

- the application on the computing device constructing the send item;

- one of the application and the attestation unit monitoring for pre-determined indicia that can be employed to detect that a minimum effort is in fact expended to construct the send item;

- the attestation unit authenticating the application to impart trust thereto;

- one of the application and the attestation unit, upon a command being issued to send the constructed send item to the recipient, constructing a send attestation to accompany the send item, the send attestation being based on the monitored indicia and the authentication of the application and thereby describing effort expended to construct the send item;

- one of the attestation unit and the application packaging the constructed send attestation with the constructed send item; and

- one of the attestation unit and the application sending the packaged send item and send attestation to the recipient.

2. The method of claim 1 describing user interaction in combination with sending the send item from the application of the computing device to the recipient, the computing device having the attestation unit thereon for attesting to trustworthiness, the method comprising:

- the application on the computing device facilitating a user in constructing the send item;

- one of the application and the attestation unit monitoring for pre-determined indicia that can be employed to detect that the user is in fact expending effort to construct the send item;

- the attestation unit authenticating the application to impart trust thereto;

- one of the application and the attestation unit, upon the user commanding the application to send the constructed send item to the recipient, constructing a send attestation to accompany the send item, the send attestation being based on the monitored indicia and the authentication of the application and thereby describing the user interaction;

one of the attestation unit and the application packaging the constructed send attestation with the constructed send item; and

one of the attestation unit and the application sending the packaged send item and send attestation to the recipient.

3. The method of claim 1 comprising an electronic mail application on the computing device constructing an electronic mail message to be sent to the recipient.

4. The method of claim 1 comprising a requesting application on the computing device constructing a request to be sent to the recipient.

5. The method of claim 1 comprising one of the application and the attestation unit monitoring for pre-determined indicia comprising at least one of keyboard activity, tablet activity, mouse activity, and lack of a run script by which activity of the application is controlled.

6. The method of claim 1 comprising one of the application and the attestation unit monitoring for pre-determined indicia comprising at least one of a minimum construction time for constructing the send item and a maximum number of send items sent per unit time.

7. The method of claim 1 comprising the attestation unit authenticating the application by reviewing a digital certificate proffered thereby.

8. The method of claim 1 wherein the computing device includes hardware and resources, the method further comprising the attestation unit authenticating at least some of the hardware and/or resources of the computing device that are used in constructing the send item.

9. The method of claim 8 comprising the attestation unit authenticating each piece of the hardware and/or resources by reviewing a digital certificate proffered thereby.

10. The method of claim 1 comprising one of the application and the attestation unit, determining based on the monitored indicia whether predetermine requirements have been met and if so constructing the send attestation.

11. The method of claim 1 comprising constructing the send attestation to include:

a statement describing the application and information relating to the application; and

a statement describing the send item and information relating to the send item including information relating to at least a portion of the monitored indicia.

12. The method of claim 11 wherein the computing device includes hardware and resources, the method further comprising the attestation unit authenticating at least some of the hardware and/or resources of the computing device that are used in constructing the send item, the method further comprising constructing the send attestation to include a statement describing the hardware and/or resources and information relating to such hardware and/or resources.

13. The method of claim 1 comprising packaging the constructed send attestation with the constructed send item by appending the send attestation to the send item, signing the packaged send item/send attestation based on a key of the attestation unit to form a digital signature, and appending the digital signature to the packaged send item/send attestation.

14. A method of verifying a minimum expended effort in combination with a send item received by a recipient from an application of a computing device, the send item being in a package with a send attestation based on monitored indicia

that can be employed to detect that a minimum effort was in fact expended to construct the send item and an authentication of the application and thereby describing the expended effort, the method comprising:

receiving the package with the send item and the send attestation;

verifying at least one signature included within the package;

examining the send attestation of the package in view of a pre-determined policy to decide whether to honor the send item, the policy detailing the minimum expended effort, whereby each aspect of policy can be measured as against information obtained from the send attestation; and

honoring the send item if the policy is in fact satisfied by the send attestation, and thereby accepting and acting upon the send item.

15. The method of claim 14 for verifying user interaction in combination with the send item received by the recipient from the application of the computing device, the send item being in the package with the send attestation based on the monitored indicia that can be employed to detect that a user in fact expended effort to construct the send item and the authentication of the application and thereby describing the user interaction, the method comprising:

receiving the package with the send item and the send attestation;

verifying at least one signature included within the package;

examining the send attestation of the package in view of a pre-determined policy to decide whether to honor the send item, whereby each aspect of policy can be measured as against information obtained from the send attestation; and

honoring the send item if the policy is in fact satisfied by the send attestation, and thereby accepting and acting upon the send item.

16. The method of claim 15 comprising receiving the package with the send item comprising a request originating by way of an intermediary that is to be rewarded therefor, and dishonoring the send item if it is determined that the intermediary sent the request without verified user interaction.

17. The method of claim 14 further comprising dishonoring the send item if the policy is not in fact satisfied by the send attestation, and thereby not accepting and acting upon the send item, and returning to the computing device a denial message.

18. The method of claim 14 further comprising dishonoring the send item if the policy is not in fact satisfied by the send attestation, and thereby not accepting and acting upon the send item, and notifying a denial filter of same, whereby the denial filter would then filter out further send items from the computing device.

19. The method of claim 14 further comprising dishonoring the send item if the policy is not in fact satisfied by the send attestation, and thereby not accepting and acting upon the send item, and adding the computing device to a denial list, whereby further send items from the computing device would be treated differently based on being on such list.

20. The method of claim 14 comprising receiving the package with the send item comprising an electronic mail message.

21. The method of claim 14 comprising receiving the package with the send item comprising a request.

22. The method of claim 14 comprising receiving the package with the send attestation comprising indicia monitored during construction of the send item, the indicia including at least one of keyboard activity, tablet activity, mouse activity, and lack of a run script by which activity of the application is controlled.

23. The method of claim 14 comprising receiving the package with the send attestation comprising indicia monitored during construction of the send item, the indicia including at least one of a minimum construction time for constructing the send item and a maximum number of send items sent per unit time.

24. The method of claim 14 comprising receiving the package with the send attestation including:

a statement describing the application and information relating to the application; and

a statement describing the send item and information relating to the send item including information relating to at least a portion of the monitored indicia.

25. The method of claim 24 wherein the computing device includes hardware and resources, the method comprising receiving the package with the send attestation further including a statement describing the hardware and/or resources and information relating to such hardware and/or resources.

26. The method of claim 14 comprising receiving the package with the send attestation appended to the send item, and an appended digital signature based on the packaged send item/send attestation.

* * * * *