Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2515711 C 2014/03/18

(11)(21) 2 515 711

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(22) Date de dépôt/Filing Date: 2005/08/11

(41) Mise à la disp. pub./Open to Public Insp.: 2006/03/15

(45) Date de délivrance/Issue Date: 2014/03/18

(30) Priorité/Priority: 2004/09/15 (US10/941,594)

(51) Cl.Int./Int.Cl. *H04L 12/16* (2006.01),
G06F 9/445 (2006.01), *H04L 9/00* (2006.01)

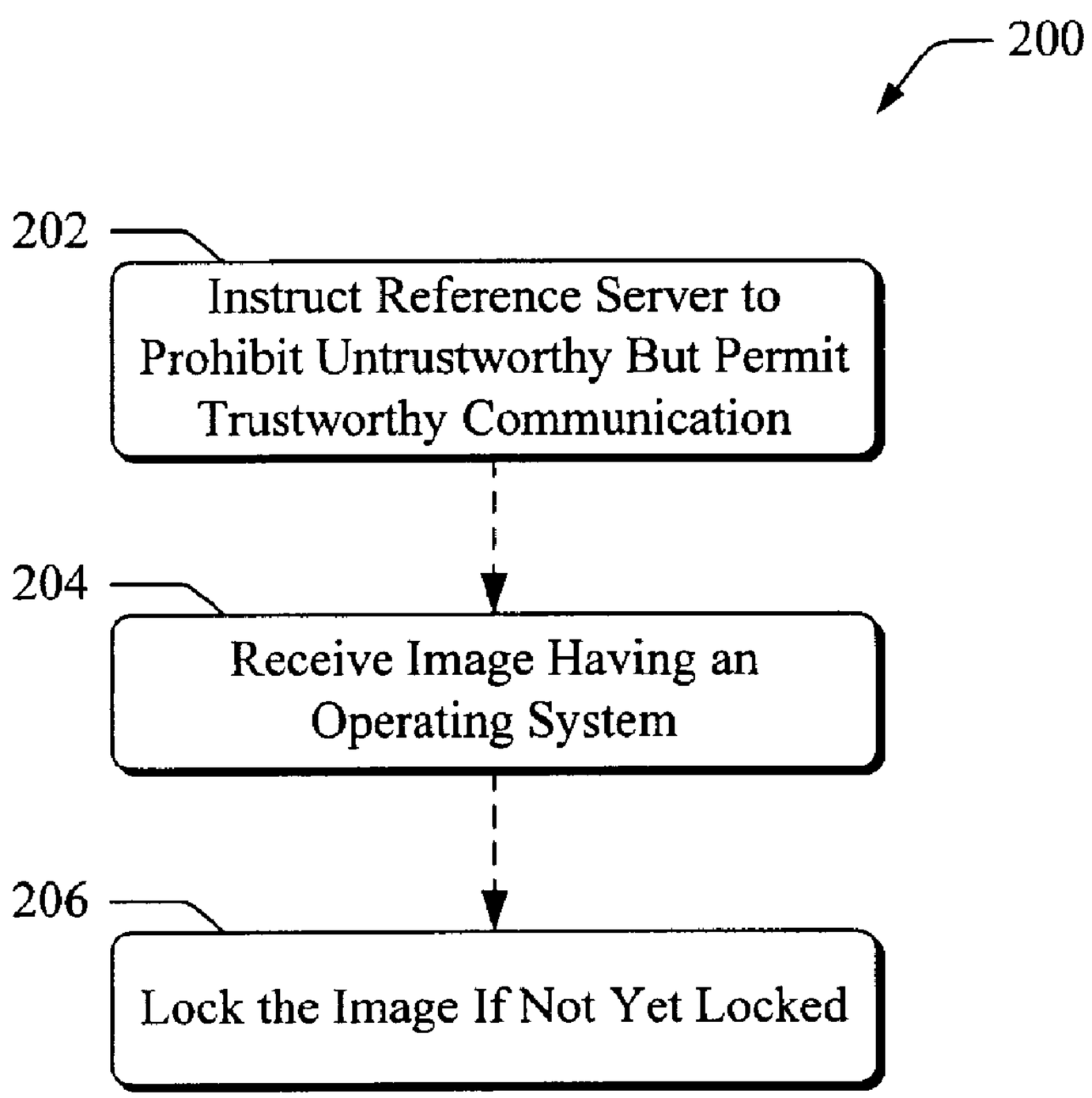
(72) Inventeurs/Inventors:
HOLLADAY, MARTIN L., US;
KARKI, MUKESH, US;
PARTHASARATHY, NARAYANAN, US

(73) Propriétaire/Owner:
MICROSOFT CORPORATION, US

(74) Agent: SMART & BIGGAR

(54) Titre : DISTRIBUTION ET RECEPTION DE LOGICIELS SUR UN RESEAU SUSCEPTIBLE DE COMMUNICATION MALICIEUSE

(54) Title: DEPLOYING AND RECEIVING SOFTWARE OVER A NETWORK SUSCEPTIBLE TO MALICIOUS COMMUNICATION



(57) Abrégé/Abstract:
Systems and/or methods that enable secure deployment and/or receipt of an operating system and updates for the operating system to a bare computer across a network susceptible to malicious communication are described. These systems and/or

CA 2515711 C 2014/03/18

(11)(21) 2 515 711

(13) C

(57) Abrégé(suite)/Abstract(continued):
methods can, in one embodiment, securely deploy an image having an operating system and enable secure receipt of an update for the operating system, both via a network susceptible to malicious communication. They can also, in another embodiment, enable a bare computer added to a network to have an operating system deployed to it and updated via the network before the bare computer is subjected to malicious code communicated over the network.

51331-281

ABSTRACT

Systems and/or methods that enable secure deployment and/or receipt of an operating system and updates for the operating system to a bare computer across a network susceptible to malicious communication are described. These systems and/or methods can, in one embodiment, securely deploy an image having an operating system and enable secure receipt of an update for the operating system, both via a network susceptible to malicious communication. They can also, in another embodiment, enable a bare computer added to a network to have an operating system deployed to it and updated via the network before the bare computer is subjected to malicious code communicated over the network.

51331-281

Deploying and Receiving Software Over a Network Susceptible to Malicious Communication

TECHNICAL FIELD

This invention relates to deploying and receiving software over a network.

BACKGROUND

One of the quickest and easiest ways to add a new, bare server (a server not having an operating system) to a network is to plug it into the network and use a deployment server on the network to deploy an image of the operating system to the bare server. The bare server can save this image to its hard disk drive or equivalent storage and then reboot. Once it reboots, it can be running with the newly deployed operating system.

Operating systems deployed to bare servers with an image are often out of date, however; they need current updates to be optimally secure. A server with an out-of-date operating system, if it is linked to the network, can acquire these updates through the network, usually from an Internet site or an intranet server having current updates.

But the network, even if it is an intranet, may be susceptible to malicious communication, such as a virus or other network-based attack. Because of this, the server often cannot acquire these updates before being attacked by malicious code via the network. In the amount of time between when the server is first running with its operating system on the network and when it has downloaded and installed current updates, malicious code like a virus or Trojan horse can attack the server. This is a real danger, as many malicious programs take less than a second to

corrupt a server running an out-of-date operating system. The MS Blaster virus, for instance, can corrupt a server without an appropriate software update within tenths of a second.

To partially combat this problem, a bare server can be connected to a deployment server without being connected to a network, such as by manually plugging a cable into both servers. Through this cable, the deployment server can deploy an image having an operating system to the bare server. The server can then be rebooted with the operating system. Once this is done, updates can be installed, usually by hand with compact disks, to make the operating system optimally secure. Once updated, the server can then be plugged into the network. This partial solution may reduce the server's vulnerability to attack, but it is time consuming. An information technology specialist can spend many hours connecting bare servers directly to a deployment server, deploying images, installing updates, disconnecting the servers from the deployment server, and then connecting them to the network.

Also to partially combat this problem, the operating system and updates can be manually installed on a bare server, usually with many compact disks, prior to connecting the server to the network. Manually installing an operating system and updates, however, is also time consuming and tedious; it can takes hours for each server.

There is, therefore, a need for a secure way to deploy an operating system and updates to a server over a network that is susceptible to malicious communication.

SUMMARY

According to one aspect of the present invention, there is provided a method comprising: receiving, by a deployment server, a locked image having an operating system and security settings, the security settings being configured to prohibit unsolicited communication via a network that is susceptible to malicious communication from other than a secure source or via a secure port, the security settings including a setting prohibiting communication with any port other than a port used by the deployment server; editing, by the deployment server, the security settings of the locked image to further configure the security settings; and securely deploying, by the deployment server, the locked image to a bare computer via the network.

According to another aspect of the present invention, there is provided a system comprising at least one processor, and one or more computer-readable storage media having processor-executable instructions stored thereon that are capable of being executed by the at least one processor, the processor-executable instructions adapted to direct the at least one processor to configure a computer to receive the locked image and to deploy the locked image, by performing the method as described above or below.

According to still another aspect of the present invention, there is provided a method comprising: receiving, by a bare computer, a locked image having an operating system and security settings via a network susceptible to malicious communication, the security settings being configured to effectively prohibit unsolicited and

potentially malicious communication from other than a secure source, the security settings including a setting prohibiting communication with any port other than a port used by the secure source, the security settings of the locked image further having been edited by a deployment server after creation of the locked image to further configure the security settings; booting, by the bare computer, the locked image, effective to run the operating system at the security settings; receiving, by the bare computer, an update to the operating system from the secure source; and applying, by the bare computer, the update to the operating system.

According to yet another aspect of the present invention, there is provided a system comprising at least one processor, and one or more computer-readable storage media having processor-executable instructions stored thereon that are capable of being executed by the at least one processor, the processor-executable instructions adapted to direct the at least one processor to configure a computer to receive the locked image, boot the locked image, receive the update and apply the update, by performing the method as described above or below.

According to a further aspect of the present invention, there is provided a method comprising: securely deploying, by a deployment server, a locked image to a computer over a network susceptible to malicious communication, the locked image having one or more security settings being configured to prohibit unsolicited communication via the network from other than a secure source or via a secure port, the security settings including

a setting prohibiting communication with any port other than a port used by the deployment server, the security settings of the locked image further having been edited by the deployment server after creation of the locked image to further configure the security settings; instructing, by the deployment server, the computer to boot the locked image; instructing, by the deployment server, the computer to solicit communication to receive a software update; receiving, by the deployment server, from the computer an indication that the software update has been received; and instructing, by the deployment server, the computer to permit potentially malicious communication over the network wherein potentially malicious communication comprises unsolicited communication.

According to yet a further aspect of the present invention, there is provided a system comprising at least one processor, and one or more computer-readable storage media having processor-executable instructions stored thereon that are capable of being executed by the at least one processor, the processor-executable instructions adapted to direct the at least one processor to configure a computer to deploy the locked image and to instruct the computer of the method as described above or below.

According to still a further aspect of the present invention, there is provided a method comprising: securely receiving a locked image having an operating system via a network susceptible to malicious communication, the locked image having one or more security settings being configured to effectively prohibit unsolicited communication via the network from other than a secure source or via a secure

port, the security settings including a setting prohibiting communication with any port other than a port used by the secure source, the security settings of the locked image further having been edited by a deployment server after creation of the locked image to further configure the security settings; booting the locked image; receiving instruction from the secure source(s) or via the secure port(s); following the instruction to securely receive a software update via the network; applying the software update effective to improve the security of the operating system; and permitting potentially malicious communication via the network wherein potentially malicious communication comprises unsolicited communication.

According to another aspect of the present invention, there is provided a system comprising at least one processor, and one or more computer-readable storage media having processor-executable instructions stored thereon that are capable of being executed by the at least one processor, the processor-executable instructions adapted to direct the at least one processor to configure a computer to receive the locked image, boot the locked image, receive instruction, and follow the instruction, by performing the method as described above or below.

According to yet another aspect of the present invention, there is provided a method comprising: editing an image having an operating system by adding or altering security settings in the image effective to prohibit unsolicited communication via a network susceptible to malicious communication other than from a secure source or via a secure port; and securely deploying the edited image

to a bare computer via the network, wherein deploying the edited image to the bare computer via the network includes instructing the bare server to alter security settings to permit communication with at least one trustworthy source.

According to another aspect of the present invention, there is provided a method comprising: editing an image having an operating system to alter a security setting for the purpose of prohibiting unsolicited communication via a network susceptible to malicious communication other than from a secure source or via a secure port; securely deploying the edited image to a computer over a network susceptible to malicious communication; instructing the computer to boot the edited image; instructing the computer to solicit communication to receive a software update; receiving from the computer an indication that the software update has been received; and instructing the computer to alter the security setting to permit potentially malicious communication over the network.

According to still another aspect of the present invention, there is provided a method comprising: enabling a bare computer capable of communicating through a network that is susceptible to malicious communication to request and receive an operating system and security settings via the network, whereby the security settings are configured to instruct the bare computer to effectively prohibit receiving potentially malicious communication other than from a secure source via the network, wherein potentially malicious communications comprises unsolicited communications; enabling the bare computer to receive, prior to the bare computer being subjected to potentially malicious

communication via the network, an update to the operating system via the network; enabling the bare computer, without user interaction, to commence potentially malicious communication over the network after the bare computer has applied the update to the operating system.

According to yet another aspect of the present invention, there is provided a method comprising: enabling a bare computer to request an operating system through a network susceptible to malicious communication; enabling the bare computer to automatically receive, through the network susceptible to malicious communication, the operating system and instructions, the instructions directing the bare computer to run in a secure mode that effectively prohibits the computer from receiving malicious communications via the network, wherein malicious communications comprises unsolicited communications; enabling the bare computer to automatically communicate via the network that the operating system has been installed; enabling the bare computer to automatically receive, through the network susceptible to malicious communication, an update to the operating system; enabling the bare computer to automatically apply the update prior to the bare computer being subjected to potentially malicious communication via the network; enabling the bare computer to automatically communicate via the network that the update to the operating system has been installed; and enabling the bare computer to automatically terminate the secure mode without user interaction and commence potentially malicious communication over the network after the bare computer has applied the update to the operating system.

According to a further aspect of the present invention, there is provided a method comprising: enabling a bare computer capable of communicating through a network that is susceptible to potentially malicious communication to request and receive an operating system and configured security settings via the network; enabling the bare computer to boot the operating system effective to run the operating system in a secure mode based on the configured security settings, wherein the secure mode effectively prohibits the bare computer from receiving unsolicited and potentially malicious communication via the network; enabling the bare computer to receive instructions via the network to securely receive an update to the operating system; enabling the bare computer to receive and install the update to the operating system via the network; enabling the bare computer to communicate via the network that the update to the operating system has been installed; and enabling the bare computer to terminate the secure mode without user interaction and commence potentially malicious communication over the network after the bare computer has applied the update to the operating system.

According to yet a further aspect of the present invention, there is provided a method comprising: receiving, by a deployment server, an image having an operating system from a reference computer; if the received image is not locked, automatically locking, by the deployment server, the received image by editing the image's security settings to add or turn on a firewall to prohibit unsolicited communications, the firewall prohibiting communication with any port other than the port used by the deployment server;

securely deploying the locked image to a computer over a network susceptible to malicious communication; instructing, by the deployment server, the computer to boot the locked image; instructing, by the deployment server, the computer to solicit communication to receive a software update; receiving, by the deployment server, from the computer an indication that the software update has been successfully applied; and instructing, by the deployment server, the computer to permit potentially malicious communication over the network by opening ports of the firewall after having received the indication.

According to still a further aspect of the present invention, there is provided the method as described above or below, further comprising the following steps performed by the computer: securely receiving the locked image having the operating system via the network susceptible to malicious communication; booting the locked image, the locked image having security settings effective to prohibit unsolicited communication other than from one or more secure sources or via one or more secure ports; receiving instruction from the secure source(s) or via the secure port(s); following the instruction to securely receive a software update via the network; applying the software update effective to improve the security of the operating system; and permitting potentially malicious communication via the network.

According to another aspect of the present invention, there is provided one or more computer-readable storage media having computer-executable instructions stored thereon that, when executed by a processor cause the processor to perform the method as described above or below.

According to yet another aspect of the present invention, there is provided a system comprising one or more computer-readable storage media having computer-executable instructions stored thereon that, when executed by a processor cause the processor to perform the method as described above or below.

Systems and/or methods ("tools") that enable secure deployment and/or receipt of an operating system and updates for the operating system to a bare computer across a network are described. In one embodiment, for instance, the tools securely deploy an image having an operating system and enable secure receipt of an update for the operating system, both via a network that is susceptible to malicious communication. In a second embodiment, for example, the tools deploy to a computer across a network an operating system that, when run by the computer, prohibits the computer from receiving malicious and/or unsolicited communications via the network. In a third embodiment, for instance, the tools enable a bare computer added to a network to have an operating system deployed to it and updated via the network before the bare computer is subjected to malicious code communicated over the network.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 illustrates an exemplary architecture having exemplary servers, a network susceptible to malicious communication, and bare computers.

Fig. 2 sets forth a flow diagram of an exemplary process for creating a locked image having an operating system.

Fig. 3 sets forth a flow diagram of an exemplary process for deploying and receiving a locked image and updates via a network susceptible to malicious communication.

The same numbers are used throughout the disclosure and figures to reference like components and features.

DETAILED DESCRIPTION

An Exemplary Architecture

Referring to Figure 1, an exemplary architecture 100 is shown having a reference server 102, a deployment server 104, an update server 106, and a server rack 108. The reference server, deployment server, and update server are shown as three separate servers, though they can be combined into one or more servers in any combination. The deployment server comprises computer-readable media capable of performing one or more of the processes described below. These media can comprise a deployment application 110 and a locking application 112, for instance. The locking application is shown as part of the deployment application, though each can be separate or combined. The update server also comprises computer-readable media, here capable of deploying software patches, fixes, and the like, such as to update an out-of-date operating system for improving its operation, e.g., its security capabilities.

Three exemplary bare computers are also shown, a bare server 114 in rack 108, a bare stand-alone server 116, and a bare desktop 118. Each of the bare computers has a software or hardware application sufficient to enable the bare computer to request, receive, and follow basic instructions, such as from the deployment application 110.

The architecture 100 communicates across a network 120. The network is a communication network susceptible to malicious communication, such as network-based attacks.

This network can comprise an intranet in communication with an insecure source, such as the Internet or a corrupted computer within the intranet capable of sending malicious code across the network.

Building a Locked Image

Referring to Figure 2, an exemplary process 200 for building a locked image is shown. This process is illustrated as a series of blocks representing individual operations or acts performed by deployment server 104, such as with locking application 112. This and other processes described herein may be implemented in any suitable hardware, software, firmware, or combination thereof. In the case of software and firmware, these processes represent sets of operations implemented as computer-executable instructions.

At block 202, deployment server 104, using locking application 112, instructs reference server 102 to prohibit communications with untrustworthy sources but permit communication with at least one trustworthy source, such as the deployment server. The prohibited communications can comprise all communications that are not solicited by the reference server or all communications, solicited or not (other than those permitted from the trustworthy source).

In one embodiment, the locking application selectively prohibits communication by instructing the reference server to enable a firewall prohibiting communication with any port other than the port used by the deployment server. In another embodiment, the locking application does so by instructing the reference server to enable one or more protocols, such as IPSec ("Internet Protocol Security"), which can prohibit communication with

any computer other than the deployment server (and, in some cases, update server 106). In both embodiments, the reference server is instructed to alter its settings to operate securely but permit communication with at least one trustworthy source.

These settings are stored in the memory of the reference server. Because of this, an image of the reference server's memory can comprise the operating system and these settings. A bare computer booting up this image can run the operating system having these settings, thereby prohibiting potentially dangerous communications but permitting communication with a trustworthy source. If the bare computer that is to receive the image is a desktop or other non-server computer, the reference server can be a reference desktop or other non-server reference computer.

At block 204, deployment server 104 receives an image having an operating system. In one embodiment, the deployment server performs blocks 204 and 206 and in another embodiment performs blocks 202 and 204, as set described below. This image can be received from the reference server of Figure 1 or another reference computer (not shown). If the image is locked, such as resulting from the actions of block 202, the deployment server does not proceed to block 206. If the image is not locked, the deployment server proceeds to block 206. In another embodiment, the deployment server waits to lock the image until after the image has been saved to the bare server but before the bare server reboots (not shown).

At block 206, the deployment server, through locking application 112, edits an image having an operating system. This editing can comprise locking the image by

altering a security setting to prohibit unsolicited communications except from at least one trustworthy source, such as deployment server 104. The prohibited communications can comprise all communications that are not solicited by the computer running the operating system or all communications, solicited or not (other than those permitted from the trustworthy source). The locking application can do so by editing the image's security setting(s) to add or turn on a firewall like the firewall described in block 202. The locking application can also do so, for instance, by editing the image's security setting(s) to comprise IPSec protocols, such as those described in block 202. Thus, the locking application locks the image to prohibit potentially dangerous communications by a computer running the software in the image but permit communication with a trustworthy source.

Deploying a Locked Image and Updating an Operating System

Referring to Figure 3, an exemplary process 300 for securely deploying, via a network susceptible to malicious communication, an image having an operating system and enabling secure receipt of an update for the operating system is shown. This process is illustrated as a series of blocks representing individual operations or acts performed by deployment server 104, such as with deploying application 110. An exemplary process 302 for securely receiving the locked image and updates to the operating system is also shown. Process 302 is illustrated as a series of blocks representing operations or acts performed by or to bare server 114.

At block 304, a bare computer is connected to network 120. In the ongoing embodiment, bare server 114 is

plugged into the network via rack 108, though other bare computers can instead be connected to the network, such as stand-alone server 116 or desktop 118.

At block 306, the bare server communicates across the network, requesting an operating system. Without an operating system, the bare server often is not yet vulnerable to malicious code on the network.

At block 308, deployment server 104 receives the request for an operating system. At block 310, the deployment server, through deployment application 110, securely deploys a locked image having an operating system to the bare server. At this block, the deployment server can, in some embodiments, also deploy software updates. The locked image can be the result of the process 200. In the ongoing embodiment, the locked image is one that, when run by the bare server (which will then no longer be bare), will not permit receipt of unsolicited communication from any source other than the deployment server or any port other than the port used by the deployment server.

At block 312, the bare server securely receives the locked image via the network and saves it to memory. By securely receiving the locked image, the bare server can receive the locked image without its being subject to malicious communication during transmission. Secure communication of this locked image can also prohibit it from being intercepted or monitored by a third party. In one embodiment, the bare server also receives updates with or as part of the locked image. At block 314, the bare server communicates that it has received the locked image. At block 316, the deployment server receives the communication from the bare server indicating that it has received the

locked image. At block 318, the deployment server, through the deployment application, instructs the bare server to boot the locked image.

At block 320, the bare server reboots, thereby running the image with the operating system and its secure settings. The bare server, now no longer bare as it has an operating system, is running in a secure mode. The bare server, because of settings and/or software in the image, can prohibit untrustworthy or potentially malicious communications. The bare server can operate securely even though it is connected to network 120 and potentially is operating with an out-of-date operating system that could otherwise be vulnerable to malicious communication sent over the network.

At block 322, bare server 114 informs the deployment server that the operating system is running and/or that the boot was successful.

At block 324, deployment server 104 receives this information. At block 326, the deployment server, through deployment application 110, instructs the bare server to securely receive and/or install updates. In the ongoing embodiment, the deployment server instructs the bare server to initiate communication with update server 106. In another embodiment, the deployment server securely sends updates to the bare server's operating system and instructs it to add these updates without use of a separate update source like the update server. In still another embodiment, the updates are received along with or as part of the image received at block 312 and sent at block 310. In this embodiment, the deployment server instructs the bare server to install the already received updates. The updates

received in any of these embodiments can be effective to update the operating system or other software on the bare server, and can comprise software patches, fixes, and the like. These updates can improve resistance to various malicious code later received by the bare server, described in greater detail below.

At block 328, the bare server receives the instruction to securely receive updates. In the ongoing embodiment, the bare server receives the instruction from the deployment server.

At block 330, the bare server initiates secure communication to securely receive updates. In the ongoing embodiment, the bare server solicits communication from update server 106. The bare server's security settings are configured to prevent receipt of unsolicited communication, but the bare server is permitted to solicit communication from the update server. By so doing, updates and other information from the solicited update server can be received by the bare server running the operating system. Other, unsolicited information, can be refused by the bare server because of its security settings, thereby protecting the bare server from unsolicited, malicious code while enabling the bare server to receive updates.

At block 332, the bare server securely receives and applies updates to its operating system. These updates can be received via the network from the update server solicited at block 330 or from the deployment server directly, for instance. This secure receipt of updates enables the bare server to have an updated operating system via a network that is susceptible to malicious communication

without first being vulnerable to malicious code communicated over the network.

At block 334, the bare server communicates that it has updated its operating system. At block 336, the deployment server receives this communication.

At block 338, the deployment server instructs the bare server to commence potentially malicious communication. Because the operating system is updated, the bare server is better capable of defending itself against malicious code and attacks communicated across the network. In one embodiment, the deployment server sends and/or instructs the bare server to install a firewall or IPSec protocols to further secure the bare server's operations before commencing potentially malicious communication.

At block 340, the bare server commences potentially malicious communication over the network, such as by commencing a production mode of operation. The bare server can do so by opening particular ports, for instance. If the bare server is to be a webserver, for instance, it can open port 80 to enable it to communicate with other servers across the Internet.

In the ongoing embodiment, most if not all of the acts of the deployment server and the deployment application can be performed automatically and without user interaction. This enables a user to connect a bare server or other bare computer to a network and, without further interaction, have the bare server operating with an updated operating system without having to subject the bare server to malicious code via the network before the operating system is updated.

CONCLUSION

The above-described tools enable secure deployment and/or receipt of an operating system and updates across a network that can be susceptible to malicious communication. Although the invention has been described in language specific to structural features and/or methodological acts, it is to be understood that the invention defined in the appended claims is not necessarily limited to the specific features or acts described. Rather, the specific features and acts are disclosed as exemplary forms of implementing the claimed invention.

51018-46

CLAIMS:

1. A method comprising:

receiving, by a deployment server, a locked image having an operating system and security settings, the security settings being configured to prohibit unsolicited communication via a network that is susceptible to malicious communication from other than a secure source or via a secure port, the security settings including a setting prohibiting communication with any port other than a port used by the deployment server;

editing, by the deployment server, the security settings of the locked image to further configure the security settings; and

securely deploying, by the deployment server, the locked image to a bare computer via the network.

2. The method of claim 1, further comprising:

instructing the bare computer to securely receive a software update.

3. The method of claim 2, wherein the software update is capable of improving the operating system's resistance to malicious code.

4. The method of claim 2, further comprising receiving an indication that the software update has been applied and instructing the bare computer to commence communication via the network.

5. The method of claim 1, further comprising instructing a reference server having the operating system

to prohibit unsolicited communication via the network other than from the secure source or via the secure port.

6. The method of claim 5, wherein the act of instructing the reference server comprises instructing the reference server to enable a firewall.

7. The method of claim 1, wherein the bare computer comprises a bare server.

8. A system comprising at least one processor, and one or more computer-readable storage media having processor-executable instructions stored thereon that are capable of being executed by the at least one processor, the processor-executable instructions adapted to direct the at least one processor to configure a computer to receive the locked image and to deploy the locked image, by performing the method recited in claim 1.

9. A method comprising:

receiving, by a bare computer, a locked image having an operating system and security settings via a network susceptible to malicious communication, the security settings being configured to effectively prohibit unsolicited and potentially malicious communication from other than a secure source, the security settings including a setting prohibiting communication with any port other than a port used by the secure source, the security settings of the locked image further having been edited by a deployment server after creation of the locked image to further configure the security settings;

booting, by the bare computer, the locked image, effective to run the operating system at the security settings;

receiving, by the bare computer, an update to the operating system from the secure source; and

applying, by the bare computer, the update to the operating system.

10. The method of claim 9, wherein the security settings are effective to permit unsolicited and secure communication from a secure source or via a secure port.

11. The method of claim 10, wherein the act of receiving the update is via the network.

12. The method of claim 9, wherein the act of receiving the update comprises receiving an instruction to solicit communication from an update source and soliciting the update source for the update.

13. The method of claim 9, further comprising:

permitting unsolicited and potentially malicious communication via the network.

14. The method of claim 13, wherein the act of permitting comprises altering the security settings to permit unsolicited and potentially malicious communication.

15. The method of claim 9, wherein the acts of receiving the locked image, booting the locked image, receiving the update, and applying the update are performed without user interaction.

16. A system comprising at least one processor, and one or more computer-readable storage media having processor-executable instructions stored thereon that are capable of being executed by the at least one processor, the processor-executable instructions adapted to direct the at

least one processor to configure a computer to receive the locked image, boot the locked image, receive the update and apply the update, by performing the method recited in claim 9.

17. A method comprising:

securely deploying, by a deployment server, a locked image to a computer over a network susceptible to malicious communication, the locked image having one or more security settings being configured to prohibit unsolicited communication via the network from other than a secure source or via a secure port, the security settings including a setting prohibiting communication with any port other than a port used by the deployment server, the security settings of the locked image further having been edited by the deployment server after creation of the locked image to further configure the security settings;

instructing, by the deployment server, the computer to boot the locked image;

instructing, by the deployment server, the computer to solicit communication to receive a software update;

receiving, by the deployment server, from the computer an indication that the software update has been received; and

instructing, by the deployment server, the computer to permit potentially malicious communication over the network wherein potentially malicious communication comprises unsolicited communication.

18. The method of claim 17, further comprising instructing a reference server to prohibit unsolicited communication via the network other than from a secure source or via a secure port and receiving the locked image from the reference server.

19. The method of claim 18, wherein the act of instructing the reference server comprises instructing the reference server to enable a firewall.

20. The method of claim 18, wherein the act of instructing the reference server comprises instructing the reference server to add IPSec protocols.

21. The method of claim 17, wherein the locked image is capable of prohibiting communication sent across the network that is unsolicited and potentially malicious.

22. The method of claim 17, wherein the locked image is capable of prohibiting unsolicited communication other than from a source from which the locked image was deployed.

23. The method of claim 17, wherein the software update is effective to improve an operating system's resistance to malicious code.

24. The method of claim 17, wherein the computer comprises a bare server.

25. The method of claim 17, wherein the act of instructing the computer to solicit communication comprises instructing the computer to solicit communication from an update server over the network.

26. The method of claim 17, wherein the indication indicates that the software update has been successfully applied.

27. The method of claim 17, wherein the act of receiving and the acts of instructing are communicated via the network.

28. The method of claim 17, wherein the network comprises an intranet capable of communicating with the internet.

29. A system comprising at least one processor, and one or more computer-readable storage media having processor-executable instructions stored thereon that are capable of being executed by the at least one processor, the processor-executable instructions adapted to direct the at least one processor to configure a computer to deploy the locked image and to instruct the computer of the method recited in claim 17.

30. A method comprising:

securely receiving a locked image having an operating system via a network susceptible to malicious communication, the locked image having one or more security settings being configured to effectively prohibit unsolicited communication via the network from other than a secure source or via a secure port, the security settings including a setting prohibiting communication with any port other than a port used by the secure source, the security settings of the locked image further having been edited by a deployment server after creation of the locked image to further configure the security settings;

booting the locked image;

receiving instruction from the secure source(s) or via the secure port(s);

following the instruction to securely receive a software update via the network;

applying the software update effective to improve the security of the operating system; and

permitting potentially malicious communication via the network wherein potentially malicious communication comprises unsolicited communication.

31. The method of claim 30, wherein the locked image and the instruction are received from a deployment server via the network.

32. The method of claim 30, wherein at least four of the acts of securely receiving, booting, receiving instruction, following the instruction, applying, and permitting are performed without human interaction.

33. A system comprising at least one processor, and one or more computer-readable storage media having processor-executable instructions stored thereon that are capable of being executed by the at least one processor, the processor-executable instructions adapted to direct the at least one processor to configure a computer to receive the locked image, boot the locked image, receive instruction, and follow the instruction, by performing the method recited in claim 30.

34. A method comprising:

editing an image having an operating system by adding or altering security settings in the image effective to prohibit unsolicited communication via a network susceptible to malicious communication other than from a secure source or via a secure port; and

securely deploying the edited image to a bare computer via the network, wherein deploying the edited image to the bare computer via the network includes instructing the bare server to alter security settings to permit communication with at least one trustworthy source.

35. The method of claim 34, further comprising:

instructing the bare computer to securely receive a software update from the at least one trustworthy source.

36. The method of claim 35, wherein the software update is capable of improving the operating system's resistance to malicious code.

37. The method of claim 35, further comprising receiving an indication that the software update has been applied and instructing the bare computer to commence potentially malicious communication via the network.

38. The method of claim 34, wherein the act of editing comprises enabling operation of a firewall in the image.

39. The method of claim 34, wherein the act of editing comprises adding one or more security protocols to the image.

40. The method of claim 34, wherein the bare computer comprises a bare server.

41. One or more computer-readable storage media having computer-executable instructions stored thereon that when executed by a processor cause the processor to perform the method recited in claim 34.

42. A system comprising means for performing the method recited in claim 34.

43. A method comprising:

editing an image having an operating system to alter a security setting for the purpose of prohibiting unsolicited communication via a network susceptible to malicious communication other than from a secure source or via a secure port;

securely deploying the edited image to a computer over a network susceptible to malicious communication;

instructing the computer to boot the edited image;

instructing the computer to solicit communication to receive a software update;

receiving from the computer an indication that the software update has been received; and

instructing the computer to alter the security setting to permit potentially malicious communication over the network.

44. The method of claim 43, wherein the act of editing comprises adding or turning on a firewall.

45. The method of claim 43, wherein the act of editing comprises adding or turning on IPSec protocols.

46. The method of claim 43, wherein the altered security setting is capable of prohibiting communication to the computer sent across the network that is unsolicited and potentially malicious.

47. The method of claim 43, wherein the altered security setting is capable of prohibiting unsolicited communication to the computer other than from a source from which the edited image was deployed.

48. The method of claim 43, wherein the software update is effective to improve the operating system's resistance to malicious code.

49. The method of claim 43, wherein the computer comprises a bare server.

50. The method of claim 43, wherein the act of instructing the computer to solicit communication comprises instructing the computer to solicit communication from an update server over the network.

51. The method of claim 43, wherein the indication indicates that the software update has been successfully applied.

52. The method of claim 43, wherein the act of receiving and the acts of instructing are communicated via the network.

53. The method of claim 43, wherein the network comprises an intranet capable of communicating with the Internet.

54. One or more computer-readable storage media having computer-executable instructions stored thereon that when

executed by a processor cause the processor to perform the method recited in claim 43.

55. A system comprising means for performing the method recited in claim 43.

56. A method comprising:

enabling a bare computer capable of communicating through a network that is susceptible to malicious communication to request and receive an operating system and security settings via the network, whereby the security settings are configured to instruct the bare computer to effectively prohibit receiving potentially malicious communication other than from a secure source via the network, wherein potentially malicious communications comprises unsolicited communications;

enabling the bare computer to receive, prior to the bare computer being subjected to potentially malicious communication via the network, an update to the operating system via the network;

enabling the bare computer, without user interaction, to commence potentially malicious communication over the network after the bare computer has applied the update to the operating system.

57. The method of claim 56, wherein the bare computer comprises a bare server.

58. The method of claim 56, wherein the operating system is received as an image.

59. The method of claim 58, wherein the image comprises the security settings capable of prohibiting the

bare computer from receiving insecure communication via the network.

60. The method of claim 56, wherein the update is capable of modifying the operating system's security.

61. The method of claim 56, further comprising:

enabling the bare computer to apply the update prior to the bare computer being subjected to potentially malicious communication via the network.

62. The method of claim 61, wherein the acts of enabling are performed without user interaction.

63. One or more computer-readable storage media having computer-executable instructions stored thereon that, when executed by a processor cause the processor to perform the method as recited in claim 56.

64. A system comprising one or more computer-readable storage media having computer-executable instructions stored thereon that, when executed by a processor cause the processor to perform the method as recited in claim 56.

65. A method comprising:

enabling a bare computer to request an operating system through a network susceptible to malicious communication;

enabling the bare computer to automatically receive, through the network susceptible to malicious communication, the operating system and instructions, the instructions directing the bare computer to run in a secure mode that effectively prohibits the computer from receiving

malicious communications via the network, wherein malicious communications comprises unsolicited communications;

enabling the bare computer to automatically communicate via the network that the operating system has been installed;

enabling the bare computer to automatically receive, through the network susceptible to malicious communication, an update to the operating system;

enabling the bare computer to automatically apply the update prior to the bare computer being subjected to potentially malicious communication via the network;

enabling the bare computer to automatically communicate via the network that the update to the operating system has been installed; and

enabling the bare computer to automatically terminate the secure mode without user interaction and commence potentially malicious communication over the network after the bare computer has applied the update to the operating system.

66. The method of claim 65, wherein the act of enabling the bare computer to receive the operating system is performed without the bare computer being subjected to potentially malicious communication via the network.

67. The method of claim 65, wherein the operating system is received as an image.

68. The method of claim 67, wherein the image comprises security settings capable of prohibiting the bare

computer from receiving potentially malicious communication via the network.

69. The method of claim 65, wherein the bare computer comprises a bare server.

70. The method of claim 65, wherein the update is capable of modifying the operating system's security.

71. The method of claim 65, wherein the acts of enabling are performed without user interaction.

72. One or more computer-readable storage media having computer-executable instructions stored thereon that when executed by a processor cause the processor to perform the method as recited in claim 65.

73. A system comprising one or more computer-readable storage media having computer-executable instructions stored thereon that, when executed by a processor cause the processor to perform the method as recited in claim 65.

74. A method comprising:

enabling a bare computer capable of communicating through a network that is susceptible to potentially malicious communication to request and receive an operating system and configured security settings via the network;

enabling the bare computer to boot the operating system effective to run the operating system in a secure mode based on the configured security settings, wherein the secure mode effectively prohibits the bare computer from receiving unsolicited and potentially malicious communication via the network;

51018-46

enabling the bare computer to receive instructions via the network to securely receive an update to the operating system;

enabling the bare computer to receive and install the update to the operating system via the network;

enabling the bare computer to communicate via the network that the update to the operating system has been installed; and

enabling the bare computer to terminate the secure mode without user interaction and commence potentially malicious communication over the network after the bare computer has applied the update to the operating system.

75. The method of claim 74, wherein the operating system is received as an image.

76. The method of claim 74, wherein the update is capable of modifying the operating system's security.

77. The method of claim 74, wherein the enabling is performed without user interaction.

78. A method comprising:

receiving, by a deployment server, an image having an operating system from a reference computer;

if the received image is not locked, automatically locking, by the deployment server, the received image by editing the image's security settings to add or turn on a firewall to prohibit unsolicited communications, the firewall prohibiting communication with any port other than the port used by the deployment server;

securely deploying the locked image to a computer over a network susceptible to malicious communication;

instructing, by the deployment server, the computer to boot the locked image;

instructing, by the deployment server, the computer to solicit communication to receive a software update;

receiving, by the deployment server, from the computer an indication that the software update has been successfully applied; and

instructing, by the deployment server, the computer to permit potentially malicious communication over the network by opening ports of the firewall after having received the indication.

79. The method of claim 78, wherein the reference computer is a reference server, the method further comprising instructing the reference server to prohibit unsolicited communication via the network other than from a secure source or via a secure port and receiving the locked image from the reference server.

80. The method of claim 79, wherein the act of instructing the reference server comprises instructing the reference server to enable a firewall.

81. The method of claim 79, wherein the act of instructing the reference server comprises instructing the reference server to add IPSec protocols.

82. The method of claim 78, wherein the locked image is capable of prohibiting communication sent across the network that is unsolicited and potentially malicious.

83. The method of claim 78, wherein the locked image is capable of prohibiting unsolicited communication other than from a source from which the locked image was deployed.

84. The method of claim 78, wherein the software update is effective to improve an operating system's resistance to malicious code.

85. The method of claim 78, wherein the computer comprises a bare computer.

86. The method of claim 78, wherein the computer comprises a bare server.

87. The method of claim 78, wherein the act of instructing the computer to solicit communication comprises instructing the computer to solicit communication from an update server over the network.

88. The method of claim 78, wherein the act of receiving and the acts of instructing are communicated via the network.

89. The method of claim 78, wherein the network comprises an intranet capable of communicating with the Internet.

90. The method of one of claims 78 to 89, further comprising the following steps performed by the computer:

securely receiving the locked image having the operating system via the network susceptible to malicious communication;

booting the locked image, the locked image having security settings effective to prohibit unsolicited communication other than from one or more secure sources or via one or more secure ports;

receiving instruction from the secure source(s) or via the secure port(s);

following the instruction to securely receive a software update via the network;

applying the software update effective to improve the security of the operating system; and

permitting potentially malicious communication via the network.

91. The method of claim 90, wherein the locked image and the instruction are received from the deployment server via the network.

92. The method of claim 90, wherein at least four of the acts of securely receiving, booting, receiving instruction, following the instruction, applying, and permitting are performed without human interaction.

93. The method of claim 90, wherein the act of receiving the update comprises receiving an instruction to solicit communication from an update source and soliciting the update source for the update.

94. The method of claim 90, wherein the act of permitting comprises

permitting unsolicited and potentially malicious communication via the network.

95. The method of claim 94, wherein the act of permitting comprises altering the security setting to permit unsolicited and potentially malicious communication.

96. The method of claim 90, wherein the acts of receiving the locked image, booting the locked image, receiving the update, and applying the update are performed without user interaction.

97. A system comprising means for performing the method recited in one of claims 78 to 96.

98. One or more computer-readable storage media having computer-executable instructions stored thereon that when executed by a processor cause the processor to perform the method recited in one of claims 78 to 96.

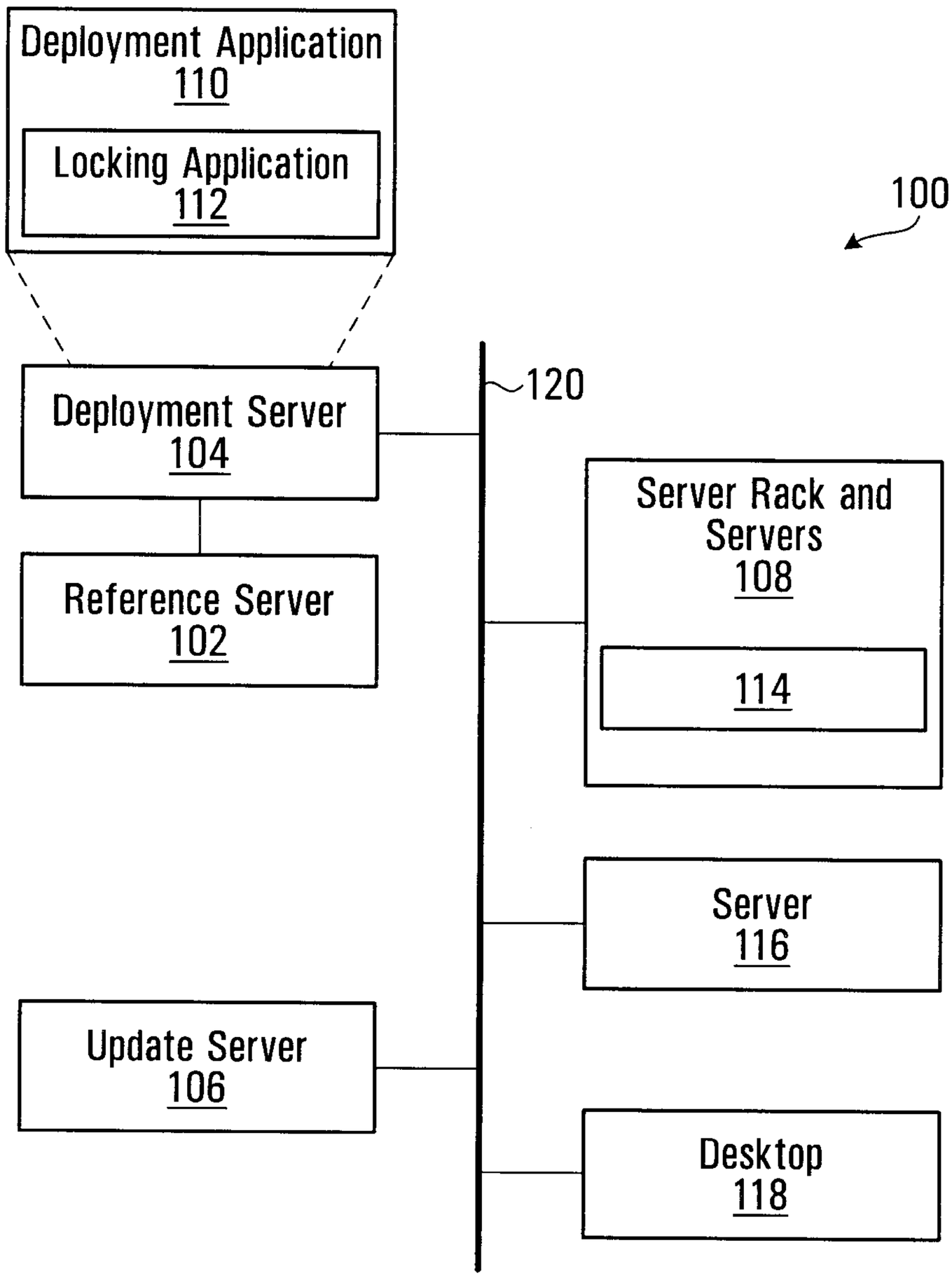

Deployment Application
110
Locking Application
112
100
Deployment Server
104
120
Reference Server
102
Server Rack and
Servers
108
114
Server
116
Update Server
106
Desktop
118

FIG. 1

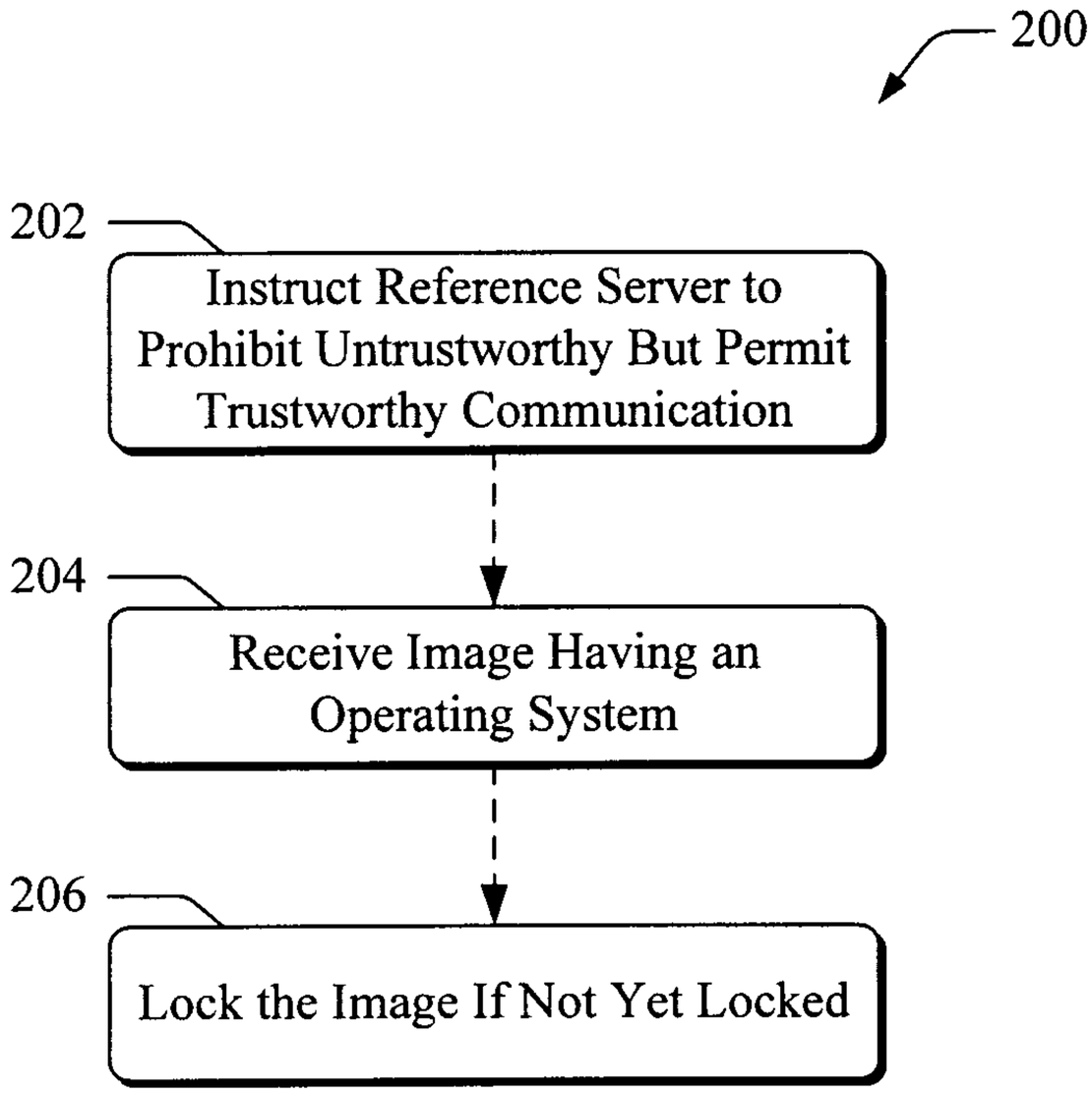

200
202
Instruct Reference Server to Prohibit Untrustworthy But Permit Trustworthy Communication
204
Receive Image Having an Operating System
206
Lock the Image If Not Yet Locked

Fig. 2

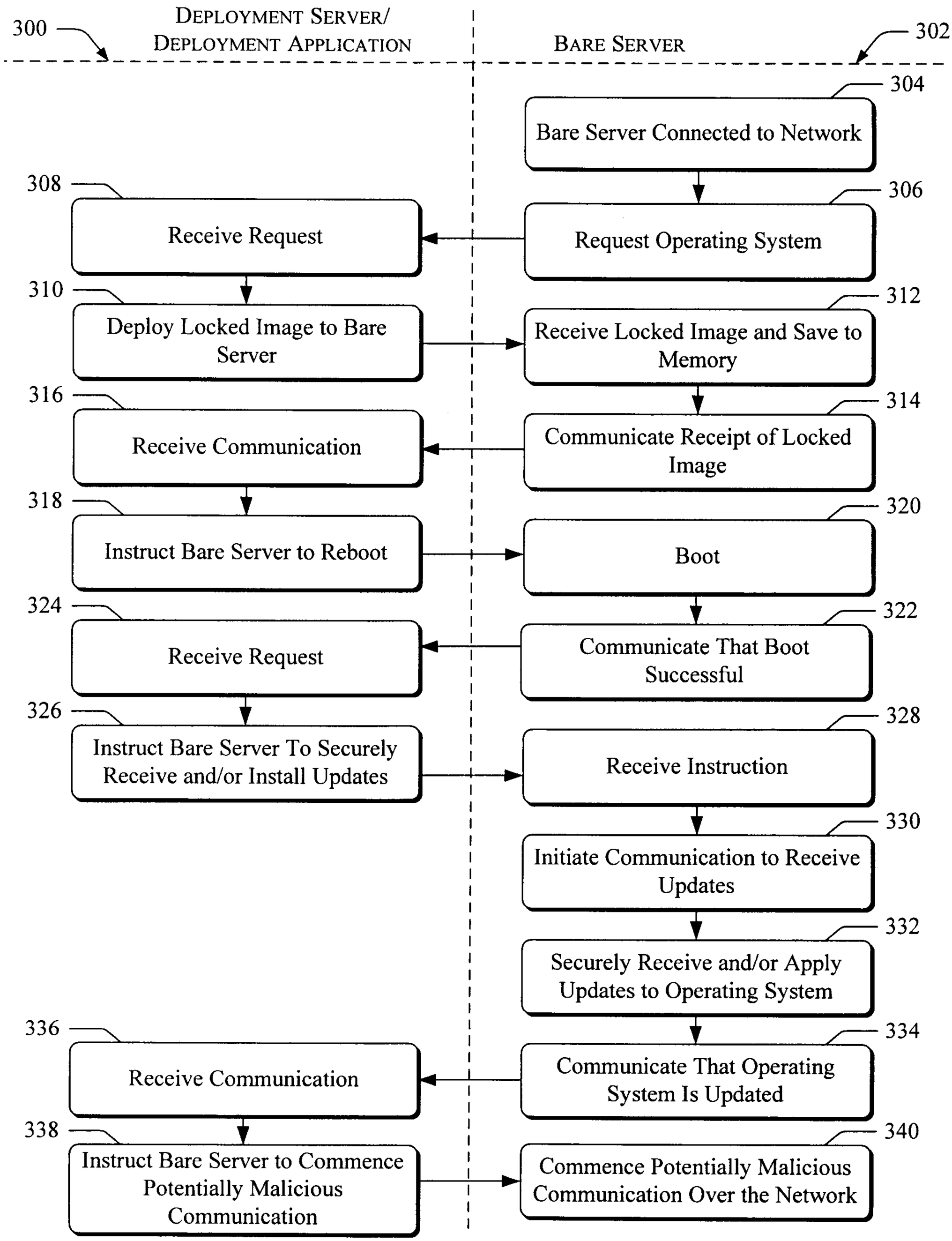
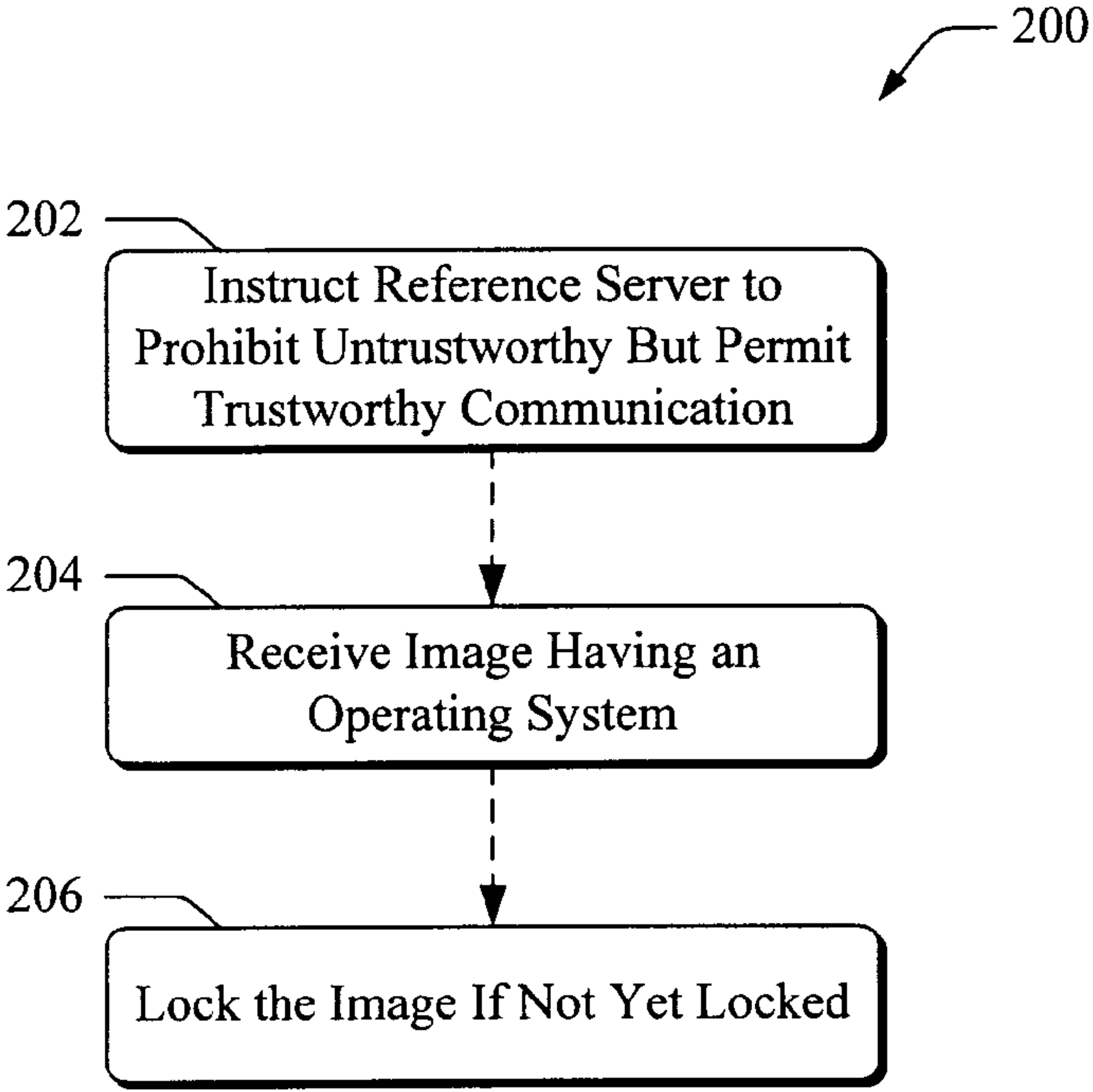

300
Deployment Server/
Deployment Application
Bare Server
302
304
Bare Server Connected to Network
306
Request Operating System
308
Receive Request
310
Deploy Locked Image to Bare Server
312
Receive Locked Image and Save to Memory
314
Communicate Receipt of Locked Image
316
Receive Communication
318
Instruct Bare Server to Reboot
320
Boot
322
Communicate That Boot Successful
324
Receive Request
326
Instruct Bare Server To Securely Receive and/or Install Updates
328
Receive Instruction
330
Initiate Communication to Receive Updates
332
Securely Receive and/or Apply Updates to Operating System
334
Communicate That Operating System Is Updated
336
Receive Communication
338
Instruct Bare Server to Commence Potentially Malicious Communication
340
Commence Potentially Malicious Communication Over the Network

Fig. 3


200
202
Instruct Reference Server to Prohibit Untrustworthy But Permit Trustworthy Communication
204
Receive Image Having an Operating System
206
Lock the Image If Not Yet Locked