(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 October 2019 (17.10.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/199374 A1

(51) International Patent Classification:
G06F 21/30 (2013.01)

(21) International Application Number:
PCT/US2019/017416

(22) International Filing Date:
11 February 2019 (11.02.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
IN201841013555 09 April 2018 (09.04.2018) IN

(71) Applicant: **HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.** [US/US]; 10300 Energy Drive, Spring, Texas 77389 (US).

(72) Inventors: **YALAMARTHI, Balaji**; Pritech Park- SEZ, Sarjapur, Block 6A, Bellandur, Outer Ring Rd, Village, Sarjapur, Bangalore 560103 (IN). **AMARENDRA, Shakti**; Pritech Park- SEZ, Sarjapur, Block 6A, Bellandur, Outer Ring Rd, Village, Sarjapur, Bangalore 560103 (IN). **SHARANABASAPPA,**; Pritech Park- SEZ, Sarjapur, Block 6A, Bellandur, Outer Ring Rd, Village, Sarjapur, Bangalore 560103 (IN). **AGRAWAL, Vasu**; Ground, 1, 2, 3, 8th Floor, Block 6A, Pritech Park SEZ, Survey No. 51-64/4, Marathahalli Outer Ring Road, Bellandur, Village, Sarjapur, Bangalore 560103 (IN). **GHALI, Anusha**; Pritech Park- SEZ, Sarjapur, Block 6A, Bellandur, Outer Ring Rd, Village, Sarjapur, Bangalore 560103 (IN).

(74) Agent: **SORENSEN, C. Blake,**; HP Inc., 3390 E. Harmony Road, Mail Stop 35, Fort Collins, Colorado 80528 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,

(54) Title: SECURE FILE ACCESS

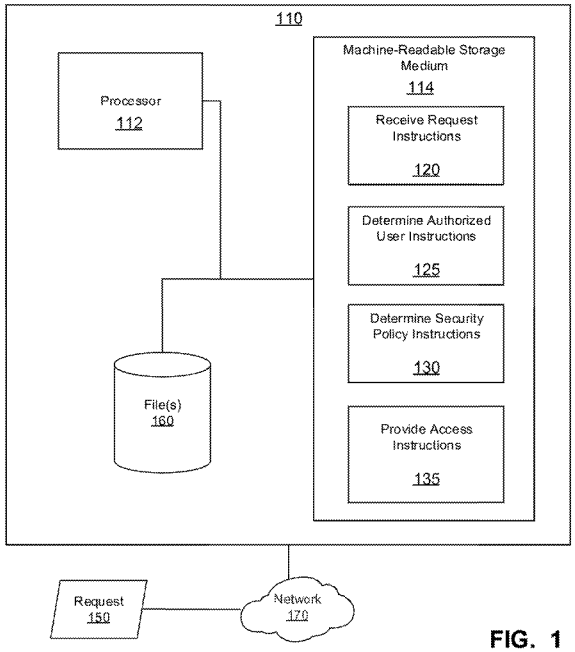

FIG. 1

(57) Abstract: Examples disclosed herein relate to receiving a request for a file via a network, determining whether the request for the file is associated with an authorized user for the file, in response to determining that the request for the file is associated with the authorized user for the file, determining whether the request for the file complies with a security policy associated with the network, and in response to determining that the request for the file complies with the security policy associated with the network, providing access to the file to the authorized user.

WO 2019/199374 A1

[Continued on next page]

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*

Published:

— *with international search report (Art. 21(3))*

SECURE FILE ACCESS

Background

[0001] Multi-function devices often combine different components such as a printer, scanner, and copier into a single device. Such devices frequently enable network access to their functions, such as scanning documents to a file that may then be retrieved from other network-connected devices, such as smartphones and computers.

Brief Description of the Drawings

[0002] FIG. 1 is a block diagram of an example computing device for providing secure access to a file.

[0003] FIG. 2 is a block diagram of an example system for providing secure access to a file.

[0004] FIG. 3 is a flowchart of an example method for providing secure access to a file.

[0005] Throughout the drawings, identical reference numbers designate similar, but not necessarily identical, elements. The figures are not necessarily to scale, and the size of some parts may be exaggerated to more clearly illustrate the example shown. Moreover the drawings provide examples and/or implementations consistent with the description; however, the description is not limited to the examples and/or implementations provided in the drawings.

Detailed Description

[0006] Most multi-function-print devices (MFPs) provide several features, including an option to scan a physical document and send it to a user-specified email address. Other options may include printing, copying, faxing, document assembly, etc. The scanning portion of an MFP may comprise an optical assembly located within a sealed enclosure. The sealed enclosure may have a scan window through which the optical assembly can scan a document, which may be placed on a flatbed and/or delivered by a sheet feeder mechanism.

[0007] The optical assembly may capture an image of the document for storage in a digital file format. For example, the optical assembly may comprise a light source and an image sensor. The image sensor may be a linear image sensor or an array of image sensors that spans a width of a document to be scanned. The light source may be a linear light source, such as a florescent tube, an array of light sources, such as a series of light emitting diodes (LEDs), or a light guide with a point light source or sources. The light source may emit light through the scan window onto the medium to be scanned while the image sensor captures light reflected by the medium through the scan window. A lens or array of lenses, such as a rod lens array, may be provided to focus light on the image sensor.

[0008] Once captured, the image of the document may be stored in a digital file format such as a portable document format (PDF), a tagged image file format (TIFF), JPEG, etc. Such files may be stored on the MFP and/or in another storage device, such as a network-attached storage, external drive, cloud service, etc. The file may be accessed in numerous ways, such as emailing to a user and/or retrieved by following a web-based link to the file's storage location.

[0009] The convenience of scanning to email, however, has an inherent security loophole as a rogue user in an office might scan a confidential document and send it to an outside email address, such as a personal account or a competitor. Further, some MFPs support network-connectivity such that applications may request retrieval of scanned documents from rogue client devices, such as those located outside an enterprise's secure internal network.

[0010] Security policies may be put into place to prevent such a rogue user from capturing confidential information. A security policy may be used to examine various criteria around operations to transfer data, such as a file associated with a scanner's output, and determine whether any of those criteria comprise a risk of improper exposure. For example, attempts to transfer a file via email may be examined to determine whether the recipient email address is associated with an approved domain name and/or a specific approved user. For another example, requests to transfer the file may determine whether the request is received from and/or comprises a request to deliver the file to an approved IP address, such as an IP address associated with an approved network. Such approved networks may comprise, for example, specifically delimited subnets and/or networks whose IP addresses resolve to approved domains via a reverse-DNS (Domain Name Service) lookup operation. In some implementations, the operation to transfer the file may only be approved under a security policy if the requestor and/or recipient are associated with an IP address that resolves to the same domain name as an IP address of the MFP that scanned the file.

[0011] FIG. 1 is a block diagram of an example computing device 110 for providing secure access to a file. Computing device 110 may comprise a processor 112 and a non-transitory, machine-readable storage medium 114. Storage medium 114 may comprise a plurality of processor-executable instructions, such as receive request instructions 120, determine authorized user instructions 125, determine security policy compliance instructions 130, and provide access instructions 135. In some implementations, instructions 120, 125, 130, 135 may be associated with a single computing device 110 and/or may be communicatively coupled among different computing devices such as via a direct connection, bus, or network.

[0012] Processor 112 may comprise a central processing unit (CPU), a semiconductor-based microprocessor, a programmable component such as a complex programmable logic device (CPLD) and/or field-programmable gate array (FPGA), or any other hardware device suitable for retrieval and execution of instructions stored in machine-readable storage medium 114. In particular, processor 112 may fetch, decode, and execute instructions 120, 125, 130, 135.

[0013] Executable instructions 120, 125, 130, 135 may comprise logic stored in any portion and/or component of machine-readable storage medium 114 and executable by processor 112. The machine-readable storage medium 114 may comprise both volatile and/or nonvolatile memory and data storage components. Volatile components are those that do not retain data values upon loss of power. Nonvolatile components are those that retain data upon a loss of power.

[0014] The machine-readable storage medium 114 may comprise, for example, random access memory (RAM), read-only memory (ROM), hard disk drives, solid-state drives, USB flash drives, memory cards accessed via a memory card reader, floppy disks accessed via an associated floppy disk drive, optical discs accessed via an optical disc drive, magnetic tapes accessed via an appropriate tape drive, and/or other memory components, and/or a combination of any two and/or more of these memory components. In addition, the RAM may comprise, for example, static random access memory (SRAM), dynamic random access memory (DRAM), and/or magnetic random access memory (MRAM) and other such devices. The ROM may comprise, for example, a programmable read-only memory (PROM), an erasable programmable read-only memory (EPROM), an electrically erasable programmable read-only memory (EEPROM), and/or other like memory device.

[0015] Receive request instructions 120 may receive a request 150 for a file 160 via a network 170. In some implementations, the request for the file 160 may comprise a request to send the file 160 to an email address. The file 160 may comprise, for example, a scanned document file 160 captured by a printing device connected to the network. In some implementations, a plurality of files 160 may be available, stored locally on device 110 and/or accessible via network 170. Network 170 may comprise any of a number of communication types and protocols, such as ethernet, wireless, radio, cellular, Bluetooth, the Internet, etc. For example, network 170 may comprise an office intranet utilizing wireless communications and/or wired communications. In some implementations, network 170 may represent a direct communication path between a request originating device and device 110, such as a USB cable.

[0016] Request 150 may comprise information about the file 160 to be requested, a user associated with making the request 150, and a user associated with receiving the

file 160. In some examples, the user making the request 150 may be the same as the user to receive the file 160. In other examples, the user may make the request 150 for the file 160 on behalf of another recipient user.

[0017] Determine authorized user instructions 125 may determine whether the request 150 for the file 160 is associated with an authorized user for the file 160. In some implementations, instructions 125 may comprise instructions to determine whether the request 150 is received from a user identifier associated with an authorized domain name. For example, requests for file 160 may only be authorized by users having an email address and/or other identifier associated with a domain name (e.g., "company.com") configured by an administrator of device 110 as authorized. The requesting user may be required to enter their email address and/or other credentials, such as by logging in to device 110 and/or another application that may create the request, so as to provide the domain name.

[0018] In some implementations, instructions 125 may comprise instructions to determine whether an email address of a user associated with the request 150 comprises a same domain as an email address associated with the scanned document file 160. For example, the email address may be associated with the scanned document file 160 by the printing device in conjunction with a scan operation to capture the scanned document file 160. The email address associated with the scanned file 160 may therefore be associated with an email address of a user who performed the scan operation. In such an example, instructions 125 may determine whether the email address of the user making the request 150 for the file 160 and the email address of the user responsible for creating the file 160 are associated with the same domain name.

[0019] Determine security policy compliance instructions 130 may, in response to determining that the request 150 for the file 160 is associated with the authorized user for the file 160, determine whether the request 150 for the file 160 complies with a security policy associated with the network. In some implementations, instructions 130 may comprise instructions to determine whether the request 150 is received from an approved network address and/or to determine whether the request 150 is associated with a network address sharing a domain name with the network. For example, request 150 may be received from an application connected to network 170, which may

comprise an internal corporate network. Instructions 130 may determine that the IP address from which request 150 is received is in the same internal network, such as in the same private subnet, as device 110. In some implementations, instructions 130 may comprise instructions to determine whether an email address in a request 150 to send the file 160 to the email address comprises an authorized domain name.

[0020] In some implementations, the instructions to determine whether the request 150 is received from the network address sharing the domain name with the network comprise instructions to perform a reverse lookup on the network address and a reverse lookup on a second network address associated with the file 160. For example, request 150 may come in via the Internet from a public IP address. By performing a reverse-DNS lookup on the public IP address, instructions 130 may determine whether the public IP address is associated with an approved domain name. The IP address may be routed through a reverse Domain Name System (DNS) lookup operation to identify a domain name associated with the IP address using pointer (PTR) records maintained according to the DNS standard. Once the domain name has been identified, instructions 130 may determine whether that domain name, wholly and/or partially, is approved for requesting and/or receiving the file 160. For example, the security policy may require that the reverse domain name at least partially match the domain name associated with a reverse DNS lookup of the IP address associated with device 110. In an example, device 110 may result in a reverse domain name lookup of "printer77.site7.company.com" while the request may be received from an IP address resolving, via reverse lookup, to "user54321.mobileapps.site4.company.com". The security policy may be configured to require only that the "company.com" portion of the domain names match and/or may require that further portions of the domain name match. In this example, the security policy may determine that a request from "*.site4.company.com" is not allowed to request files from a device with a partial domain name of "*.site7.company.com".

[0021] Provide access instructions 135 may, in response to determining that the request 150 for the file 160 complies with the security policy associated with the network, provide access to the file 160 to the authorized user. For example, providing access may comprise allowing the user to retrieve the file to another device, such as by

email, network transfer, and/or direct connection (e.g., to a USB drive). For another example, providing access may comprise allowing the user to print a copy of the file.

[0022] FIG. 2 is a block diagram of an example apparatus 200 for providing secure access to a file 260. Apparatus 200 may comprise a multi-function printer device 202 comprising a scanner 204, a display 206 to provide a user interface 208, a storage medium 210, and a processor 212. Device 202 may comprise and/or be associated with, for example, a general and/or special purpose computer, server, mainframe, desktop, laptop, tablet, smart phone, game console, printer, multi-function device, and/or any other system capable of providing computing capability consistent with providing the implementations described herein. Device 202 may store, in storage medium 210, a request engine 220, a policy engine 225, and a file access engine 230.

[0023] Each of engines 220, 225, 230 may comprise any combination of hardware and programming to implement the functionalities of the respective engine. In examples described herein, such combinations of hardware and programming may be implemented in a number of different ways. For example, the programming for the engines may be processor executable instructions stored on a non-transitory machine-readable storage medium and the hardware for the engines may include a processing resource to execute those instructions. In such examples, the machine-readable storage medium may store instructions that, when executed by the processing resource, implement engines 220, 225, 230. In such examples, device 202 may comprise the machine-readable storage medium storing the instructions and the processing resource to execute the instructions, or the machine-readable storage medium may be separate but accessible to apparatus 200 and the processing resource.

[0024] Scanner 204 may capture a digital representation of a document in a file 260. For example, device 202 may comprise a scanner component operable to capture a digital representation of a physical document. Such a scanner component may comprise a camera and/or a sheet-fed, flat-bed, and/or drum scanner. The scanner may, for example use a charge-coupled device (CCD), a photomultiplier tube (PMT), and/or a contact image sensor (CIS) as an image sensor.

[0025] Display 206 may provide user interface 208 to receive a recipient email address for the file 260. For example, a control panel may be coupled to device 202 to

provide an electronic user interface, such as via a capacitive touch screen. The user interface may allow a user to select options for various operations on device 110 and may comprise an authentication interface that allows the user to enter credentials and/or provide some form of authentication (e.g., RFID tag, biometric scan, etc.). The user may enter a destination email address for file 260 resulting from the scanner operation.

[0026] Request engine 220 may receive a request for the file 260. .In some implementations, the request for the file 260 may comprise a request to send the file 160 to an email address. The file 260 may comprise, for example, a scanned document file 160 captured by a printing device connected to the network. In some implementations, a plurality of files 260 may be available, stored locally on device 202 and/or accessible via a network.

[0027] The request may comprise information about the file 260 to be requested, a user associated with making the request, and a user associated with receiving the file 260. In some examples, the user making the request may be the same as the user to receive the file 260. In other examples, the user may make the request for the file 260 on behalf of another recipient user.

[0028] Policy engine 225 may determine whether the request complies with a security policy, wherein the security policy comprises at least one of the following: a valid network address, a valid email address and a valid network domain name. For example, policy engine 260 may execute instructions 125 to determine whether the request for the file 260 is associated with an authorized user for the file 260 and/or determine whether the request for the file 260 complies with a security policy associated with the network.

[0029] Determine authorized user instructions 125 may determine whether the request for the file 260 is associated with an authorized user for the file 260. In some implementations, instructions 125 may comprise instructions to determine whether the request is received from a user identifier associated with an authorized domain name. For example, requests for file 260 may only be authorized by users having an email address and/or other identifier associated with a domain name (e.g., “company.com”) configured by an administrator of device 202 as authorized. The requesting user may

be required to enter their email address and/or other credentials, such as by logging in to device 202 and/or another application that may create the request, so as to provide the domain name.

[0030] In some implementations, instructions 125 may comprise instructions to determine whether an email address of a user associated with the request comprises a same domain as an email address associated with the scanned document file 260. For example, the email address may be associated with the scanned document file 260 by the printing device in conjunction with a scan operation to capture the scanned document file 260. The email address associated with the scanned file 160 may therefore be associated with an email address of a user who performed the scan operation. In such an example, instructions 125 may determine whether the email address of the user making the request for the file 260 and the email address of the user responsible for creating the file 260 are associated with the same domain name.

[0031] Determine security policy compliance instructions 130 may, in response to determining that the request for the file 260 is associated with the authorized user for the file 260, determine whether the request for the file 260 complies with a security policy associated with the network. In some implementations, instructions 130 may comprise instructions to determine whether the request is received from an approved network address and/or to determine whether the request is associated with a network address sharing a domain name with the network. For example, request may be received from an application connected to a network, which may comprise an internal corporate network. Instructions 130 may determine that the IP address from which request is received is in the same internal network, such as in the same private subnet, as device 110. In some implementations, instructions 130 may comprise instructions to determine whether an email address in a request to send the file 260 to the email address comprises an authorized domain name.

[0032] In some implementations, the instructions to determine whether the request is received from the network address sharing the domain name with the network comprise instructions to perform a reverse lookup on the network address and a reverse lookup on a second network address associated with the file 260. For example, request may come in via the Internet from a public IP address. By performing

a reverse-DNS lookup on the public IP address, instructions 130 may determine whether the public IP address is associated with an approved domain name. The IP address may be routed through a reverse Domain Name System (DNS) lookup operation to identify a domain name associated with the IP address using pointer (PTR) records maintained according to the DNS standard. Once the domain name has been identified, instructions 130 may determine whether that domain name, wholly and/or partially, is approved for requesting and/or receiving the file 260. For example, the security policy may require that the reverse domain name at least partially match the domain name associated with a reverse DNS lookup of the IP address associated with device 202. In an example, device 202 may result in a reverse domain name lookup of "printer77.site7.company.com" while the request may be received from an IP address resolving, via reverse lookup, to "user54321.mobileapps.site4.company.com". The security policy may be configured to require only that the "company.com" portion of the domain names match and/or may require that further portions of the domain name match. In this example, the security policy may determine that a request from "*.site4.company.com" is not allowed to request files from a device with a partial domain name of "*.site7.company.com".

[0033] File access engine 230 may, in response to determining that the request complies with the security policy, provide access to the file 260. For example, providing access may comprise allowing the user to retrieve the file to another device, such as by email, network transfer, and/or direct connection (e.g., to a USB drive). For another example, providing access may comprise allowing the user to print a copy of the file.

[0034] FIG. 3 is a flowchart of an example method 300 for secure access to a file. Although execution of method 300 is described below with reference to computing device 110, other suitable components for execution of method 300 may be used.

[0035] Method 300 may begin at stage 305 and advance to stage 310 where device 110 may receive a request for a file from the user. For example, receive request instructions 120 may receive a request 150 for a file 160 via a network 170. In some implementations, the request for the file 160 may comprise a request to send the file 160 to an email address. The file 160 may comprise, for example, a scanned document file 160 captured by a printing device connected to the network. In some

implementations, a plurality of files 160 may be available, stored locally on device 110 and/or accessible via network 170. Network 170 may comprise any of a number of communication types and protocols, such as ethernet, wireless, radio, cellular, Bluetooth, the Internet, etc. For example, network 170 may comprise an office intranet utilizing wireless communications and/or wired communications. In some implementations, network 170 may represent a direct communication path between a request originating device and device 110, such as a USB cable.

[0036] Request 150 may comprise information about the file 160 to be requested, a user associated with making the request 150, and a user associated with receiving the file 160. In some examples, the user making the request 150 may be the same as the user to receive the file 160. In other examples, the user may make the request 150 for the file 160 on behalf of another recipient user.

[0037] Method 300 may then advance to stage 315 where computing device 110 may determine whether the request from the user complies with a security policy for a network address associated with the request. In some implementations, determining whether the request from the user complies with the security policy for the network address associated with the request comprises determining whether the network address resolves to an approved domain name. For example, the approved domain name may comprise a domain name associated with a scanning device associated with capturing a document to store as the available file. Such a domain-name may be identified, for example, via a reverse-lookup operation on the network address of the scanning device and/or the network address associated with the request.

[0038] For example, determine security policy compliance instructions 130 may determine whether the request 150 for the file 160 complies with a security policy associated with the network. In some implementations, instructions 130 may comprise instructions to determine whether the request 150 is received from an approved network address and/or to determine whether the request 150 is associated with a network address sharing a domain name with the network. For example, request 150 may be received from an application connected to network 170, which may comprise an internal corporate network. Instructions 130 may determine that the IP address from which request 150 is received is in the same internal network, such as in the same private

subnet, as device 110. In some implementations, instructions 130 may comprise instructions to determine whether an email address in a request 150 to send the file 160 to the email address comprises an authorized domain name.

[0039] In some implementations, the instructions to determine whether the request 150 is received from the network address sharing the domain name with the network comprise instructions to perform a reverse lookup on the network address and a reverse lookup on a second network address associated with the file 160. For example, request 150 may come in via the Internet from a public IP address. By performing a reverse-DNS lookup on the public IP address, instructions 130 may determine whether the public IP address is associated with an approved domain name. The IP address may be routed through a reverse Domain Name System (DNS) lookup operation to identify a domain name associated with the IP address using pointer (PTR) records maintained according to the DNS standard. Once the domain name has been identified, instructions 130 may determine whether that domain name, wholly and/or partially, is approved for requesting and/or receiving the file 160. For example, the security policy may require that the reverse domain name at least partially match the domain name associated with a reverse DNS lookup of the IP address associated with device 110. In an example, device 110 may result in a reverse domain name lookup of "printer77.site7.company.com" while the request may be received from an IP address resolving, via reverse lookup, to "user54321.mobileapps.site4.company.com". The security policy may be configured to require only that the "company.com" portion of the domain names match and/or may require that further portions of the domain name match. In this example, the security policy may determine that a request from "*.site4.company.com" is not allowed to request files from a device with a partial domain name of "*.site7.company.com".

[0040] In response to determining that the request from the user complies with the security policy, method 300 may then advance to stage 320 where computing device 110 may provide access to the file. In some implementations, providing access to the file may comprise emailing the file to the user at an email address comprising the approved domain name. For example, provide access instructions 135 may, in response to determining that the request 150 for the file 160 complies with the security policy

associated with the network, provide access to the file 160 to the authorized user. For example, providing access may comprise allowing the user to retrieve the file to another device, such as by email, network transfer, and/or direct connection (e.g., to a USB drive). For another example, providing access may comprise allowing the user to print a copy of the file.

[0041] Method 300 may then end at stage 350.

[0042] In the foregoing detailed description of the disclosure, reference is made to the accompanying drawings that form a part hereof, and in which is shown by way of illustration how examples of the disclosure may be practiced. These examples are described in sufficient detail to allow those of ordinary skill in the art to practice the examples of this disclosure, and it is to be understood that other examples may be utilized and that process, electrical, and/or structural changes may be made without departing from the scope of the present disclosure.

What is claimed:

1. A non-transitory machine-readable storage medium having stored thereon machine-readable instructions executable to cause a processor to:

receive a request for a file via a network;

determine whether the request for the file is associated with an authorized user for the file;

in response to determining that the request for the file is associated with the authorized user for the file, determine whether the request for the file complies with a security policy associated with the network; and

in response to determining that the request for the file complies with the security policy associated with the network, provide access to the file to the authorized user.

2. The medium of claim 1, wherein the instructions to determine whether the request for the file complies with the security policy associated with the network comprise instructions to determine whether the request is received from an approved network address.

3. The medium of claim 1, wherein the instructions to determine whether the request for the file complies with the security policy associated with the network comprise instructions to determine whether the request is received from a network address sharing a domain name with the network.

4. The medium of claim 3, wherein the instructions to determine whether the request is received from the network address sharing the domain name with the network comprise instructions to perform a reverse lookup on the network address and a reverse lookup on a second network address associated with the file.

5. The medium of claim 1, wherein the request for the file comprises a request to send the file to an email address.

6. The medium of claim 5, wherein the instructions to determine whether the

request for the file complies with the security policy associated with the network comprise instructions to determine whether the email address in the request to send the file comprises an authorized domain name.

7. The medium of claim 1, wherein the instructions to determine whether the request for the file is associated with the authorized user for the file comprise instructions to determine whether the request is received from a user identifier associated with an authorized domain name.

8. The medium of claim 1, wherein the file comprises a scanned document file captured by a printing device connected to the network.

9. The medium of claim 7, wherein the instructions to determine whether the request for the file is associated with the authorized user for the file comprise instructions to determine whether an email address of a user associated with the request comprises a same domain as an email address associated with the scanned document file.

10. The medium of claim 8, wherein the email address is associated with the scanned document file by the printing device in conjunction with a scan operation to capture the scanned document file.

11. A method comprising:

receiving a request for a file from the user;

determining whether the request from the user complies with a security policy for a network address associated with the request;

in response to determining that the request from the user complies with the security policy, providing access to the file.

12. The method of Claim 11, wherein determining whether the request from the user complies with the security policy for the network address associated with the request comprises determining whether the network address resolves to an approved domain name.

13. The method of Claim 12, wherein the approved domain name comprises a domain name associated with a scanning device associated with capturing a document to store as the available file.

14. The method of Claim 12, wherein providing access to the file comprises emailing the file to the user at an email address comprising the approved domain name.

15. An apparatus, comprising:

a scanner configured to capture a digital representation of a document in a file;

a display to provide a user interface to receive a recipient email address for the file;

a storage medium to store the file; and

a processor to execute machine-readable instructions comprising:

a request engine to receive a request for the file,

a policy engine to determine whether the request complies with a security policy, wherein the security policy comprises at least one of the following: a valid network address, a valid email address and a valid network domain name, and

a file access engine to, in response to determining that the request complies with the security policy, provide access to the file.

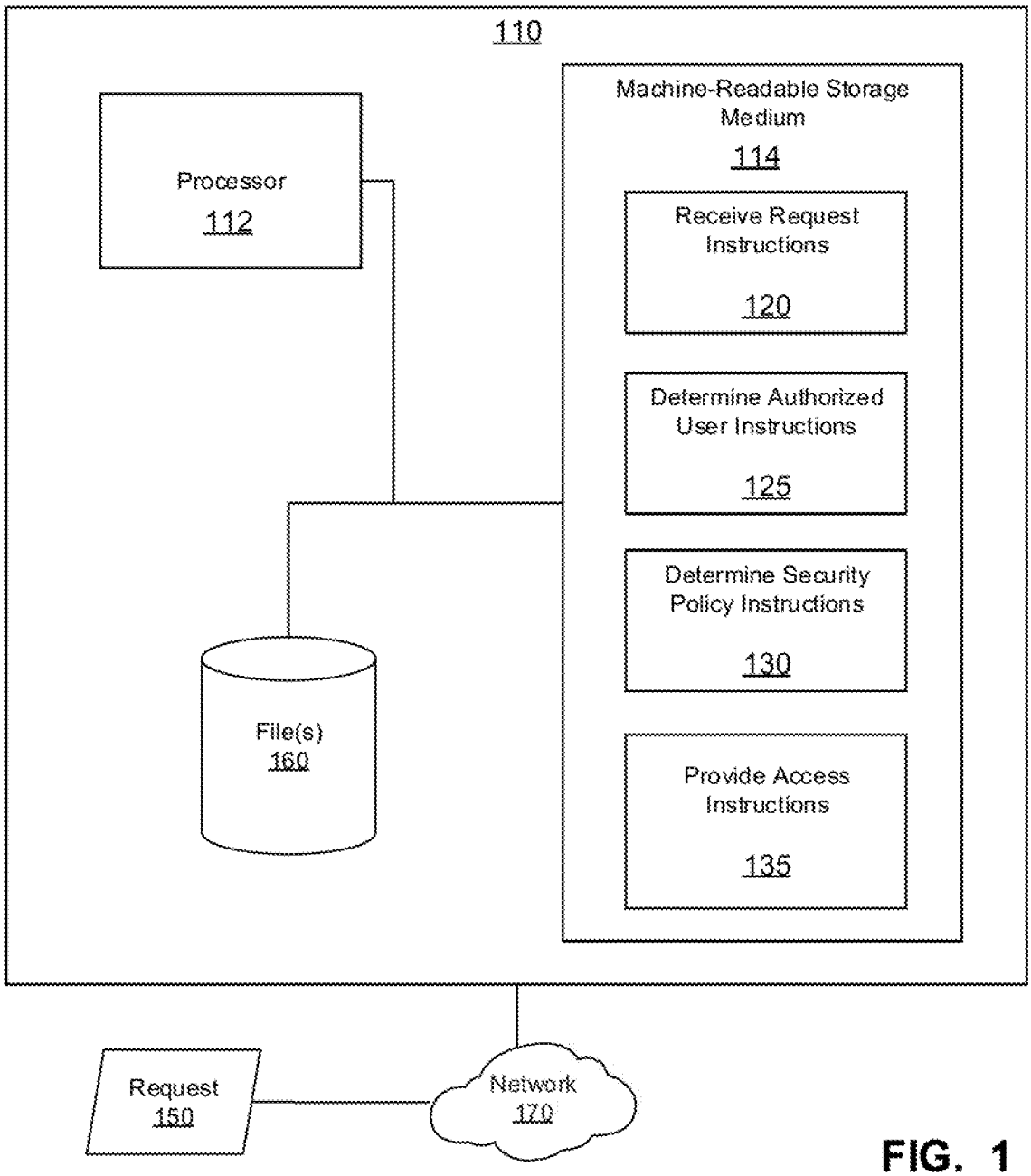
110
Processor
112
Machine-Readable Storage Medium
114
Receive Request Instructions
120
Determine Authorized User Instructions
125
Determine Security Policy Instructions
130
Provide Access Instructions
135
File(s)
160
Request
150
Network
170

FIG. 1

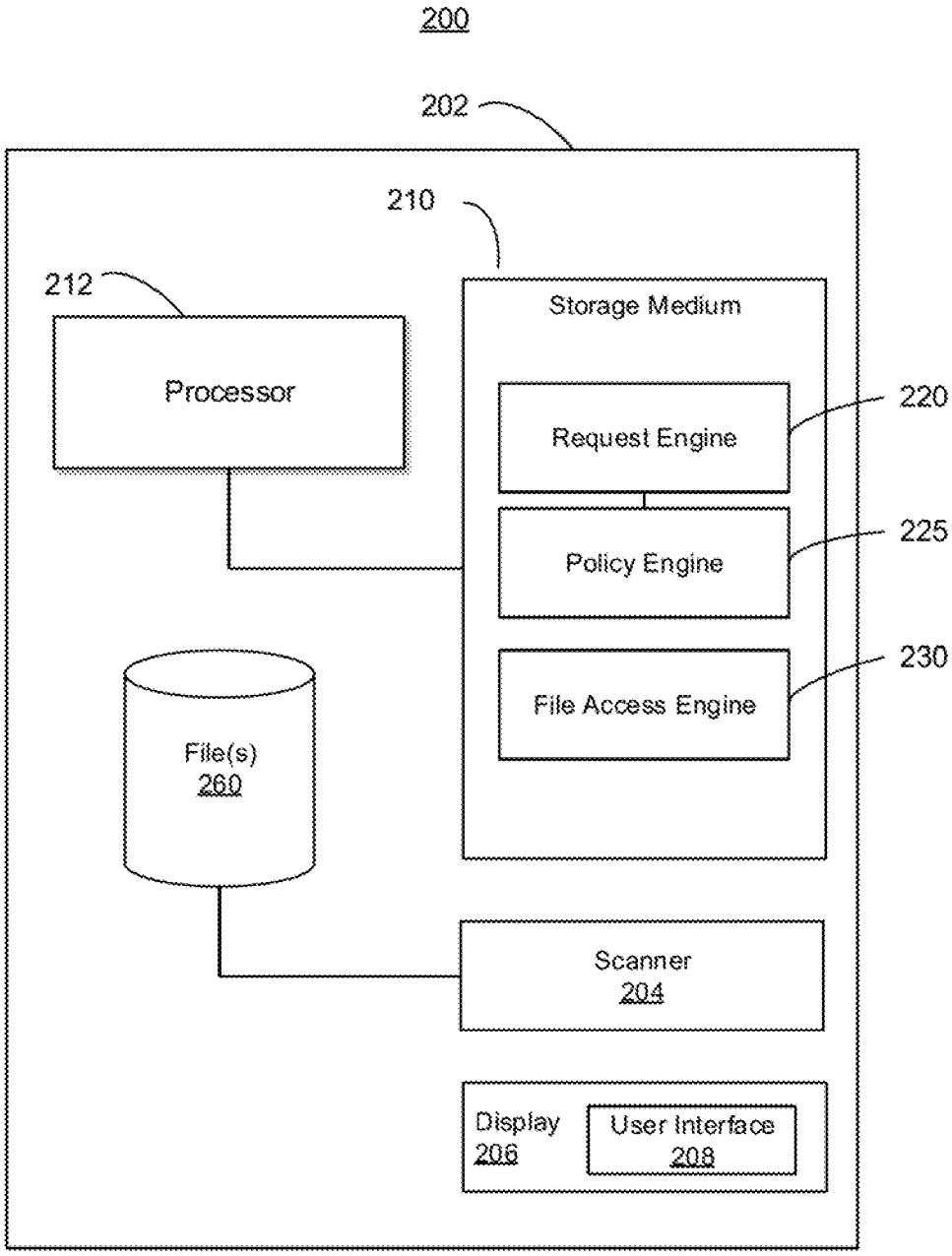
200
202
210
212
Storage Medium
Processor
Request Engine
220
Policy Engine
225
File Access Engine
230
File(s)
260
Scanner
204
Display
206
User Interface
208

FIG. 2

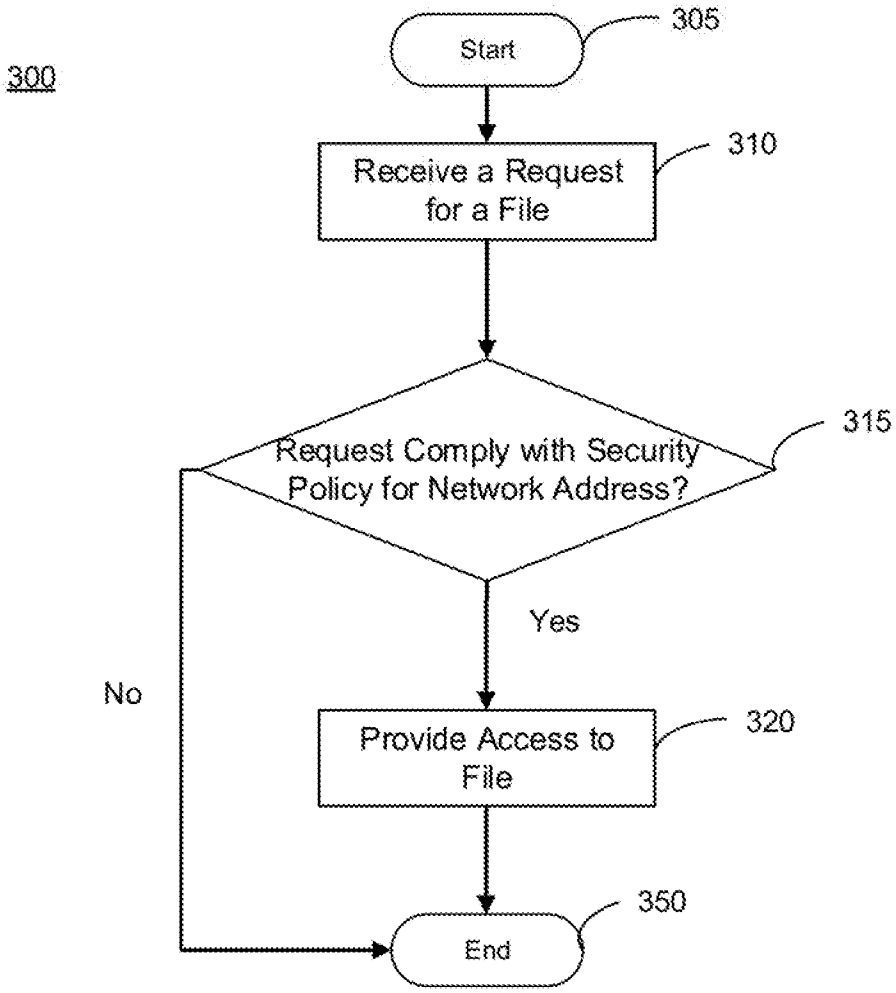
300
Start
305
Receive a Request for a File
310
Request Comply with Security Policy for Network Address?
315
Yes
No
Provide Access to File
320
End
350

FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 2019/017416

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/30 *(2013.01)*

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

PatSearch (RUPTO internal), Espacenet, DWPI,USPTO

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2015/0324235 A1 (CONTEX A/S) 12.11.2015, abstract, fig. 1, [0023],[0029],[0040]-[0043],[0059],[0066],[0067],[0070],	1-15
Y	US 2015/0229609 A1 (DANIEL CHIEN) 13.08.2015, abstract, [0043],[0063],[0068],[0069],[0083]-[0089]	1-15
A	US 2005/0216587 A1 (JOSEPH WON JOHN) 29.09.2005	1-15

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 May 2019 (25.05.2019)	23 May 2019 (23.05.2019)
Name and mailing address of the ISA/RU: Federal Institute of Industrial Property, Berezhkovskaya nab., 30-1, Moscow, G-59, GSP-3, Russia, 125993 Facsimile No: (8-495) 531-63-18, (8-499) 243-33-37	Authorized officer M. Smirnov Telephone No. (499) 240-25-91

Form PCT/ISA/210 (second sheet) (January 2015)