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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 November 2016 (24.11.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/186662 A1

(51) International Patent Classification:
G06Q 10/06 (2012.01) *G06Q 40/02* (2012.01)
G06Q 10/10 (2012.01)

(21) International Application Number:
PCT/US2015/031647

(22) International Filing Date:
19 May 2015 (19.05.2015)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **HEWLETT PACKARD ENTERPRISE DEVELOPMENT LP** [US/US]; 11445 Compaq Center Drive West, Houston, TX 77070 (US).

(72) Inventors: **KELLY, Michael**; 13600 EDS Drive, Herndon, Virginia 20171 (US). **KALIBJIAN, Jeff**; 1140 Enterprise Way, Sunnyvale, California 94089 (US).

(74) Agents: **WOODWORTH, Jeffrey C.** et al.; Hewlett Packard Enterprise, 3404 E. Harmony Road, Mail Stop 79 , Fort Collins, CO 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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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, 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))*

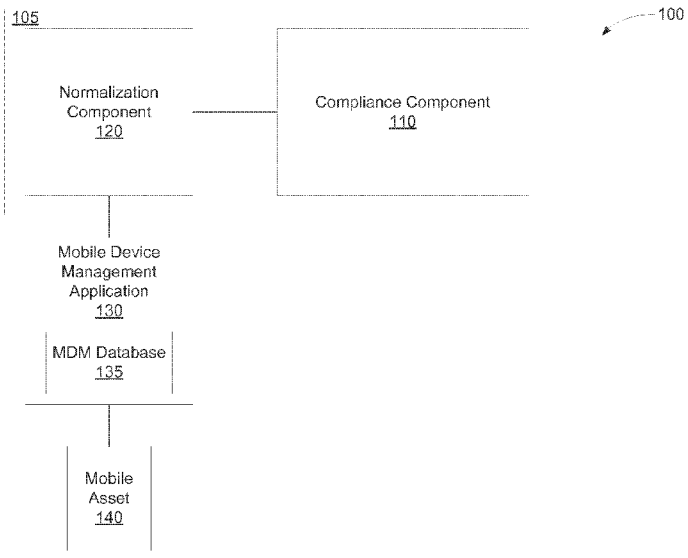
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

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

(54) Title: MOBILE ASSET COMPLIANCE EVALUATION

FIG. 1



(57) Abstract: An example system includes a normalization component. The normalization component maps configuration information for a mobile asset to a normalized schema to create normalized configuration information. The system further includes a compliance component. The compliance component evaluates conformity of the mobile asset to a standard governing information technology assets based on the normalized configuration information.

WO 2016/186662 A1

MOBILE ASSET COMPLIANCE EVALUATION

BACKGROUND

[0001] Organizations are required to comply with regulations, mandates, and policies governing their information technology (IT) assets and may face fines and penalties if they are not compliant. For example, the regulations and policies may include the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), the Sarbanes-Oxley Act, and the like. The regulations and policies provide high-level guidance that the organizations are required to follow, but the organizations must interpret the high-level guidance. Standards governing the IT assets, such as the Center for Internet Security® Benchmarks, operate at a lower level and include lists of technical controls that can be used as a baseline to measure the effectiveness of technical controls and the corresponding governing regulations, mandates, and policies. The technical controls may include specific requirements that can be measured to determine compliance with a corresponding standard. The standards may be mapped back to regulations, mandates, or policies to determine compliance with the high-level requirements of the regulations, mandates, or policies. Frameworks include overarching procedures for implementing the regulations and policies, monitoring and evaluating compliance with the standards, and using standards compliance to determine compliance with regulations and policies. For example, frameworks may include Control Objectives for Information and Related Technology (COBIT), National Institute of Standards and Technology 800-53 (NIST 800-53), and the like.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] Figure 1 is a block diagram of an example of an environment containing a system to evaluate compliance of a mobile asset with a standard.

[0003] Figure 2 is a block diagram of an example of an environment containing a system to evaluate compliance of a mobile asset with a standard and remediate vulnerabilities.

[0004] Figure 3 is a block diagram of an example of an environment containing a system to detect active vulnerabilities and threats, evaluate compliance of a mobile asset with a standard, and remediate vulnerabilities.

[0005] Figure 4 is a flow diagram of an example of a method for generating a single report of risks to mobile and fixed assets.

[0006] Figure 5 is a flow diagram of an example of a method for generating a single report of risks to mobile and fixed assets and remediating vulnerabilities.

[0007] Figure 6 is a block diagram of an example of a computer-readable medium containing instructions to map configuration information for a mobile device to a schema readable by a compliance application to determine conformity of the mobile device with a standard.

[0008] Figure 7 is a block diagram of an example of a computer-readable medium containing instructions to map identifiers, configuration information, and detected vulnerabilities and threats to a schema readable by a compliance application.

DETAILED DESCRIPTION

[0009] Technically measurable attributes of IT assets can be evaluated to determine compliance with technical controls. Compliance with the technical controls of a standard can then be mapped back to a regulation or policy. The procedures of a framework can be used to assess compliance with the standard, map the compliance with the standard back to regulations and policies, and report risks. For example, a governing regulation or policy may require enforcement of a strong password policy, and a corresponding technical control may specify a minimum password length. The IT asset configured password length can be evaluated to determine compliance with the technical control and the corresponding section of the governing regulation, mandate, or policy. If the configured password length is too short, it can be identified and reported as a finding. As used herein, an IT asset is a system or device used for organization activities, including systems and devices owned by the organization and bring-your-own-device (BYOD) systems and devices.

[0010] An organization may use governance, risk, and compliance (GRC) applications to evaluate compliance of IT assets with technical controls of a

standard governing IT assets. The GRC application may also determine compliance with governing regulations, mandates, and policies based on the compliance with the standard. The GRC application may generate reports and risk dashboards according to a framework by measuring the current state of a technical control and evaluating the implications to any corresponding and applicable regulations, mandates, or policies. The report may confirm that the organization has performed due diligence, has measured risk, and is complying with the governing regulations, mandates, policies, and standards. The report may identify risks that prevent the organization from complying with the governing regulations, mandates, policies, and standards. The GRC application may be able to evaluate the compliance of fixed IT assets (e.g., desktop computers, workstations, laptops, servers, etc.) with the governing regulations, mandates, policies, and standards. However, the GRC application is not able to assess the compliance of mobile assets, such as phones, tablets, Internet of Things devices, etc., with those governing regulations, mandates, policies, and standards.

[0011] The organization may use a mobile device management (MDM) application to manage the configurations of their mobile assets. The MDM application may be able to enforce particular configuration settings on the mobile assets. However, the MDM application is unable to measure the compliance of the mobile assets with the governing regulations, policies, mandates, and standards. The MDM application is unable to map the configuration settings to technical controls of a governing standard or evaluate the implications to regulations, mandates, or policies.

[0012] For an organization to determine compliance of mobile assets with a standard and use the determination of compliance with the standard to determine compliance with governing regulations and policies, the organization may need to check each mobile device manually and evaluate compliance with each technical control of the standard manually. For organizations with large numbers of devices, checking compliance of mobile assets may require significant amounts of time and be cost prohibitive.

[0013] Figure 1 is a block diagram of an example of an environment 100 containing a system 105 to evaluate compliance of a mobile asset 140 with a

standard. The environment 100 may include an MDM application 130, which may communicate with the mobile asset 140. In some embodiments, the system 105 may include the MDM application 130. The MDM application 130 and mobile device 140 may communicate using one or more wired or wireless networks (e.g., a local area network, a wireless local area network, a cellular network, the Internet, etc.). In the illustrated example, the MDM application 130 communicates with a single mobile asset 140, but in other examples, the MDM application 130 may communicate with a plurality of mobile assets, (e.g., tens, hundreds, thousands, or more mobile assets). The MDM application 130 may receive information about the configuration of the mobile asset 140. The MDM application 130 may store the configuration information in a local MDM database 135.

[0014] The system 105 may include a normalization component 120. The normalization component 120 may extract configuration information from the MDM application 130. In an example, the normalization component 120 may directly connect to the MDM database 135 to extract the configuration information. Alternatively, or in addition, the normalization component 120 may use an application-programming interface (API) to extract the configuration information. The MDM application 130 and normalization component 120 may mutually authenticate during extraction, and the configuration information may also be protected against modification during transfer, e.g., by using a secure channel for communication. The normalization component 120 may extract information identifying the mobile device and information that is relevant to a particular set of standards governing IT assets.

[0015] As used herein, the term 'component' refers to a combination of hardware (e.g., a processor such as an integrated circuit or other circuitry) and software (e.g., programming such as machine- or processor-executable instructions, commands, or code such as firmware, programming, or object code). A combination of hardware and software includes hardware only (i.e., a hardware element with no software elements such as an application specific integrated circuit (ASIC)), software hosted at hardware (e.g., a software module that is stored at a processor-readable memory such as random access memory (RAM),

a hard-disk or solid-state drive, resistive memory, or optical media such as a a digital versatile disc (DVD), and/or executed or interpreted by a processor), or hardware and software hosted at hardware.

[0016] The normalization component 120 may map the extracted configuration information to a normalized schema to create normalized configuration information. Database schemas for the MDM database 135 may vary among MDM applications 130. The normalization component 120 may map the configuration information to the same normalized schema regardless of the database schema of the MDM database 135 from which the configuration information was retrieved. The normalized schema may specify a predetermined structure, a predetermined organization, predetermined data formats or types, or the like for information stored by the normalization component 120. As used herein, mapping configuration information to a normalized schema is renaming, reorganizing, converting a data format or data type of, or translating data in the configuration information to conform it to the constraints of the normalized schema. Table 1 is an example of data elements that may be included in a normalized schema:

Table 1

Item	Data Type	Description
Date_Created	datetime	Date Device was created
Date_Updated	datetime	Date Device was updated
udid	char(40)	iPhone® (Apple®) unique device identifier comprised of 40 alphanumeric characters
Device_is_active	int(11)	Device is currently active
Device_is_corporate_owned	int(11)	Device is corporate owned
Version	char(100)	Version of the device
Mac_Address	char(30)	MAC Address of Wi-Fi interface
IMEI	char(30)	International mobile equipment identity; set by device manufacturer
ICCID	char(30)	Integrated circuit card identifier
Model_Number	char(30)	Device Model Number
Device_Rooted	int(11)	Device has been rooted/jail broken
Manufacturer	char(30)	Device Manufacturer
Serial_Number	char(30)	Device Serial Number
Last_Location_Timestamp	datetime	Timestamp for device

Device_Latitude	char(60)	Device Latitude
Device_Longitude	char(60)	Device Longitude
Device_Phone_Number	char(30)	Device Phone Number
Personal_Hotspot_Enabled	int(11)	Device Personal Hotspot Enabled
Data_Roaming_Enabled	int(11)	Device Data Roaming Enabled
Voice_Roaming_Enabled	int(11)	Device Roaming Enabled
Carrier_Network	char(30)	Carrier Network
Device_Blacklisted	int(11)	Device Blacklisted
Disable_Bluetooth	int(11)	Bluetooth is Disabled
Disable_Dev_Options	int(11)	Developer options is Disabled
Disable_Loc_Services	int(11)	Location Services Disabled
Passwd_Visible_Disabled	int(11)	Visible Password Disabled
Disable_Network_Notification	int(11)	Network Notification Disabled
Disable_Notifications	int(11)	Device Notifications Disabled
Disable_Wi-Fi	int(11)	Device WiFi Disabled
Enable_Airplane_Mode	int(11)	Device Airplane Mode Enabled
Enable_Encrypt phone	int(11)	Device Encryption Enabled
Enable_Lock SIM card	int(11)	Device Lock SIM Enabled
Enable_Require_alphanumeric	int(11)	Require Alpanumeric Password

[0017] A compliance component 110 (e.g., a GRC application) may receive the normalized configuration information from the normalization component 120. The compliance component 110 may receive the normalized configuration information from the normalization component 120 using a direct and secure communication channel that provides privacy and mutual authentication. The compliance component 110 may use the normalized configuration information to evaluate whether the mobile asset conforms to a standard. For example, the compliance component 110 may map the normalized configuration information to technical controls of a standard and may determine whether the normalized configuration information satisfies the technical controls of the standard.

[0018] In an example, the compliance component 110 may identify vulnerabilities or threats to the mobile asset based on its determination of whether the mobile asset complies with the standard. The compliance component 110 may also manage the security state of a fixed asset and may identify vulnerabilities or threats to the fixed asset based on the standard. The compliance component 110 may evaluate the identified vulnerabilities or threats

to the mobile and fixed assets under the same standard and may compare and contrast the vulnerabilities or threats to the mobile and fixed assets with each other. The compliance component 110 may determine the overall risk levels to the mobile and fixed assets based on the evaluation and/or the comparing and contrasting of the vulnerabilities or threats. The compliance component 110 may generate a report of risks to the mobile and fixed assets based on the evaluations of the vulnerabilities or threats to the mobile and fixed assets.

[0019] Figure 2 is a block diagram of an example of an environment 200 containing a system 205 to evaluate compliance of a mobile asset 240 with a standard and remediate vulnerabilities (e.g., vulnerabilities caused by improper configuration settings). The environment 200 may include an MDM application 230, which may communicate with the mobile asset 240. The MDM application 230 may extract configuration information from the mobile asset 240 and store the configuration information in a local MDM database 235. If configuration settings of the mobile asset 240 deviate from an intended security configuration, the MDM application 230 may be able to issue commands to the mobile device 240 to correct the improper configuration settings.

[0020] The system 205 may include a normalization component 220 to extract configuration information relevant to a standard from the MDM application 230 and to map the configuration information to a normalized schema to create normalized configuration information. The system 205 may include a compliance component 210. The compliance component 210 may evaluate conformity of the mobile asset 240 to a standard based on the normalized configuration information. The compliance component 210 may identify a vulnerability where an attribute of the mobile asset configuration is inconsistent with a compliance standard the mobile asset is being measured against.

[0021] The compliance component 210 may communicate information about the identified vulnerability to a remediation component 250. For example, the compliance component 210 may create a token containing information about the identified vulnerability. The remediation component 250 may extract pertinent vulnerability data from the information contained in the token to determine the vulnerability to be remediated. The remediation component 250 may determine a

set of notional commands to remediate the vulnerability (e.g., commands to correct a misconfiguration). The remediation component 250 may select the notional commands from a predetermined set of normalized MDM operational commands. The predetermined set of normalized MDM operational commands may be generic to a plurality of MDM applications. The notional commands may be commands to remediate a vulnerability that are generic among a plurality of MDM applications.

[0022] The remediation component 250 may then translate the set of notional commands to actual commands for the particular MDM application 230 with which it will be communicating. The remediation component 250 may communicate the actual commands to the MDM application 230. In an example, the remediation component 250 may communicate the actual commands to the MDM application 230 directly and securely using a mutually authenticated, encrypted channel. The MDM application 230 may execute the commands or cause the mobile asset 240 to execute the commands to remediate the identified vulnerability of the mobile asset 240.

[0023] The remediation component 250 may communicate with a ticketing system 260. The ticketing system 260 may track the remediation process and may provide remediation information to the remediation component 250. For example, the ticketing system 260 may communicate a token containing remediation information. The remediation component 250 may extract pertinent data, such as actions to be taken to remediate the vulnerability, from the remediation information provided by the ticketing system. The remediation component 250 may determine the set of notional commands based on the extracted remediation data.

[0024] The remediation component 250 may receive confirmation from the MDM application 230 that the actual commands have been executed successfully. In an example, the MDM application 230 may communicate the confirmation to the remediation component 250 directly and securely using a mutually authenticated, encrypted channel. The remediation component 250 may indicate to the ticketing system 260 that the vulnerability has been remediated. For example, the remediation component 250 may update a token containing

remediation information to reflect that the vulnerability has been remediated and return the token to the ticketing system 260 over a secure communications channel.

[0025] FIG. 3 is a block diagram of an example of an environment 300 containing a system 305 to detect active vulnerabilities and threats (e.g., malware, worms, viruses, and the like), evaluate compliance of a mobile asset 340 with a standard, and remediate vulnerabilities. The environment 300 may include an MDM application 330, which may communicate with the mobile asset 340. In an example, the MDM application 330 may be able to extract configuration information from the mobile asset 340 and store it in a local MDM database 335 but is not able to perform active threat detection on the mobile asset 340.

[0026] The mobile asset 340 may include an agent 345 (i.e., a threat seeking agent) to search for active vulnerabilities and threats (e.g., malware, worms, viruses, etc.) on the mobile asset 340. The system 305 may include a coordination component 370 to receive information from the agent about observed threats and vulnerabilities and to provide new threat and vulnerability descriptions to the agent 345. The threat and vulnerability descriptions may allow the agent 345 to search for and identify threats and vulnerabilities. For example, the threat and vulnerability descriptions may include virus signatures. The coordination component 370 may determine a current state of the mobile asset 340 by receiving normalized configuration information for the mobile asset 340 from a security state normalization component 320. The security state normalization component 320 may have received configuration information from the MDM application 330 and mapped it to a normalized schema to create the normalized configuration information. The coordination component 370 may retrieve or receive the normalized configuration information from the security state normalization component 320 to stay updated with the state of the mobile asset 340. The coordination component 370 may retrieve or receive information on current threats and vulnerabilities from other entities in its IT environment or from outside sources. For example, the coordination component 370 may retrieve

information on threats and vulnerabilities periodically from the National Vulnerability Database.

[0027] The coordination component 370 may decide which information it should provide to the agent 345. For example, the coordination component 370 may provide descriptions of any new threats and vulnerabilities to the agent 345. The coordination component 370 may provide the threat and vulnerability descriptions to the agent 345 in a predetermined structure. The coordination component 370 may encrypt and digitally sign the predetermined structure. The agent 345 may leave the predetermined structure encrypted and digitally signed after receiving it to prevent modification of the threat and vulnerability descriptions, for example, by a malicious application. The digital signature may prevent unauthorized entities from providing invalid threats and descriptions to the agent 345.

[0028] The coordination component 370 may include a unique, monotonically increasing number (e.g., a positive integer) in the predetermined structure to prevent replay attacks. The coordination component 370 may increase the number in each transmission of the predetermined structure to the agent 345 so the agent 345 may quickly identify if it ever has received the data contained in the structure before, which may indicate a replay attack. The coordination component 370 may include a time and date in the predetermined structure indicating when the coordination component 370 will provide updated threat and vulnerability descriptions to the agent 345. If the agent 345 does not receive the threat and vulnerability descriptions by the specified time or a predetermined time after the specified time, the agent 345 may determine that it is subject to a denial of service attack and take appropriate action. The agent 345 may signal an alarm if it did not receive the threat and vulnerability descriptions, may instruct the user to download the threat and vulnerability descriptions manually, may prevent access by the user to particular data or networks, and/or the like.

[0029] The predetermined structure may also include a priority level for each threat or vulnerability described and a central processing unit (CPU) usage goal. The agent 345 may monitor its usage of the mobile asset's CPU and attempt to use no more of the CPU than the specified goal. If the CPU usage is too high, the agent 345 may reduce its activities and may search for threats and

vulnerabilities in an order determined based on the priorities received. Accordingly, the agent 345 may minimize degradation of performance of the mobile asset 340.

[0030] The coordination component 370 may receive indications of vulnerabilities and threats observed by the agent 345. For example, the agent 345 may provide a status of its search for threats and vulnerabilities periodically, at least once per update from the coordination component 370, when the agent 345 finishes searching, and/or the like. The coordination component 370 may then provide the status and/or indications of observed vulnerabilities and threats to an active vulnerability normalization component 325. In the illustrated example, the active vulnerability normalization component 325 is separate from the security state normalization component 320, but in other examples, a single, integrated normalization component may be used. The coordination component 370 may communicate with the active vulnerability normalization component 325 over a direct, mutually authenticated, and encrypted channel. The active vulnerability normalization component 325 may map the received vulnerability and threat information to a normalized active vulnerability schema and store it as normalized vulnerability and threat information. Table 2 is an example of data elements that may be included in a normalized active vulnerability schema:

Table 2

Item	Data Type	Description
Date_Created	datetime	Date/time identified vulnerability record created
Date_Updated	datetime	Date/time identified vulnerability record updated
Devices_type	int(11)	0—infected device fixed asset; 1—infected device mobile asset
IP_Addr	char(30)	IP address of affected (if fixed asset)
IMEI	char(30)	International mobile equipment identity (if mobile asset)
Asset_Config	index	Key to asset configuration
CVE_ID	char(30)	Common vulnerability exposure identifier
CVE_BS	float	Common vulnerability scoring system base score
CVE_T	float	Common vulnerability scoring

		system temporal score
CVE_E	float	Common vulnerability scoring system environmental score
CVE_O	float	Common vulnerability scoring system overall score
GRC_Maps	index(s)	(Keys) to impacted governance mandates/regulations
Tech_Controls	index(s)	(Keys) to impacted technical controls
Threat_Status	int(11)	0—not yet remediated; 1—remediated
Remediation_Token	index(s)	Key(s) to applicable remediation token(s)
Date_Remediated	datetime	Date/time vulnerability remediated
Damage_Result	char(100)	Damage summary

[0031] The system 305 may include an active vulnerability management component 315. In the illustrated example, the active vulnerability management component 315 is separate from a compliance component 310, but in other examples, a single, integrated active vulnerability management and compliance component may be used. The active vulnerability management component 315 may receive information about observed active vulnerabilities and threats from the active vulnerability normalization component 325. The active vulnerability management component 315 may evaluate the risks associated with any threats and vulnerabilities found based on predetermined criteria, such as Common Vulnerability and Exposure (CVE) Common Vulnerability Scoring System (CVSS) base scores (e.g., from the National Vulnerability Database, Open Source Vulnerability Database, etc.), a local vulnerability score based on a vulnerability's impact on a local network and an exploitability component of a CVSS base score, or the like. If the active vulnerability management component 315 determines any vulnerabilities or threats to the mobile asset 340 have an unacceptably high level of risk, the active vulnerability management component 315 may coordinate with a remediation component 350 and ticketing system 360 to remedy the vulnerabilities or threats to the mobile asset 340. For example, the remediation component 350 may indicate to the MDM application 330 and/or the coordination component 370 actions to resolve the vulnerabilities.

[0032] Figure 4 is a flow diagram of an example of a method 400 for generating a single report of risks to mobile and fixed assets. A processor may perform the method 400. The method 400 may begin with selecting 402 configuration information from an MDM database related to a mobile asset. Configuration information that corresponds to technical controls associated with a standard governing IT assets may be selected. This may include retrieving the selected configuration information from the MDM database. For example, referring back to Figure 3, the security state normalization component 320 may select the configuration information from the MDM database.

[0033] The configuration information may be evaluated 404 based on the technical controls to determine compliance of the mobile asset with the standard. Evaluating the configuration information based on the technical controls may include mapping elements of the configuration information to individual technical controls and determining whether the mapped element satisfies the technical control to which it is mapped. Compliance of a fixed asset with the standard may be analyzed 406. Information usable to determine whether the fixed asset complies with the standard may be received directly from the fixed asset and analyzed 406 based on the technical controls.

[0034] A single report of risks for both the mobile asset and the fixed asset may be generated 408. The single report may be generated 408 based on an applicable framework. A compliance component, such as the compliance component 310 of Figure 3, may evaluate the configuration information, analyze the compliance of the fixed assets, and generate the single report of risks. The mobile and fixed assets may be evaluated based on the same technical controls and standard. Accordingly, threats and vulnerabilities may be compared across mobile and fixed assets to determine system wide compliance and risk, which can be included in the single report. The single report may provide a complete view of every asset's security posture and thereby enable security personnel to make informed, risk-based decisions about vulnerability, configuration, and threat remediation across all IT assets.

[0035] Figure 5 is a flow diagram of an example of a method 500 for generating a single report of risks to mobile and fixed assets and remediating vulnerabilities.

A processor may perform the method 500. The method 500 may begin with selecting 502 configuration information that corresponds to technical controls associated with a standard governing IT assets from an MDM database. The selected configuration information may be stored 504 in a predetermined structure, such as a structure defined by a normalized schema. Storing 504 the configuration information may include mapping the configuration information to the normalized schema so that it can be stored in the predetermined structure. In one example, the security state normalization component 320 of Figure 3 may select the configuration information and store the configuration information in the predetermined structure. The configuration information may be retrieved 506 from the predetermined structure so that it can be analyzed (e.g., retrieved by the compliance component 310 of Figure 3).

[0036] The configuration information may be evaluated 508 based on the technical controls associated with the standard governing IT assets. Compliance of a fixed asset with the standard may be analyzed 510. A single report of risks may be generated 512 based on the evaluation and analysis of the mobile and fixed assets. The compliance component 310 of Figure 3 may evaluate the configuration information, analyze the fixed assets, and generate the single report of risks. The single report of risks may explicitly include a vulnerability to be remediated, or a vulnerability to be remediated may be determined based on the single report of risks. For example, a vulnerability of a mobile asset to be remediated may be determined 514. Determining 514 a vulnerability of a mobile asset to be remediated may include receiving information identifying the vulnerability (e.g., receiving a token including information identifying the vulnerability) and determining 514 the vulnerability based on the received information. For example, the remediation component 350 of Figure 3 may receive the information identifying the vulnerability from the compliance component 310.

[0037] An indication of an action to remediate the vulnerability may be received 516, for example, from the ticketing system 360 of Figure 3 (e.g., a token including remediation information may be received). A set of notional commands to remediate the vulnerability may be determined 518. In an example, the set of

notional commands may be determined 518 based on the indication of the action to remediate the vulnerability. The set of notional commands may be selected from a predetermined set of normalized MDM operational commands. The set of notional commands may be translated 520 to actual commands for an MDM application managing the mobile asset. Translating 520 the notional commands to actual commands may include identifying the MDM application managing the mobile asset and determining commands that the identified MDM application is able to execute and that correspond to the notional commands.

[0038] The actual commands may be communicated 522 to the MDM application. A direct, mutually authenticated, encrypted channel may be established with the MDM application to communicate the actual commands. The actual commands may be digitally signed to prevent modification to the actual commands. In an example, the remediation component 350 may determine the set of notional commands, translate the set of notional commands to actual commands, and communicate the actual commands to the MDM application. Confirmation that the commands have been executed successfully may be received 524, for example, from the MDM application. The method 500 may include indicating 526 to the ticketing system that the vulnerability has been remediated (e.g., updating a token including remediation information to reflect that the vulnerability has been remediated). For example, the remediation component 350 may receive the confirmation from the MDM application and provide the indication that the vulnerability has been remediated to the ticketing system.

[0039] The methods 400, 500 may be modified to include collection of active vulnerability information (e.g., using the coordination component 370 of Figure 3). The active vulnerability information may be evaluated based on predetermined criteria, e.g., by the active vulnerability management component 315. The active vulnerability management component 315 may also evaluate active vulnerability threats of a fixed asset based on predetermined criteria. For example, the predetermined criteria may include a vulnerability score above which action will be taken to remediate the vulnerability. The compliance component 310 and the active vulnerability management component 315 may generate a single report of

risks encompassing vulnerabilities or threats from both configuration vulnerabilities or threats and active vulnerabilities or threats (e.g., the compliance component 310 and the active vulnerability management component 315 may be integrated, may communicate to generate the single report, or the like).

[0040] Figure 6 is a block diagram of an example of a computer-readable medium 600 containing instructions that, when executed by a processor 602, cause the processor 602 to map configuration information for a mobile device to a schema readable by a compliance application to determine conformity of the mobile device with a standard. The computer-readable medium 600 may be a non-transitory computer readable medium, such as a volatile computer readable medium (e.g., volatile RAM, a processor cache, a processor register, etc.), a non-volatile computer readable medium (e.g., a magnetic storage device, an optical storage device, a paper storage device, flash memory, read-only memory, non-volatile RAM, etc.), and/or the like. The processor 602 may be a general purpose processor or special purpose logic, such as a microprocessor, a digital signal processor, a microcontroller, an ASIC, a field programmable gate array (FPGA), a programmable array logic (PAL), a programmable logic array (PLA), a programmable logic device (PLD), etc.

[0041] The computer-readable medium 600 may include a relevant information identification module 610. As used herein, a module (in some examples referred to as a software module) is a set of instructions that when executed or interpreted by a processor or stored at a processor-readable medium realizes a component or performs a method. The relevant information identification module 610 may cause the processor 602 to identify configuration information that is relevant to a standard governing IT assets. The configuration information may be configuration information that is associated with a mobile asset (e.g., a mobile device) and that is stored in an MDM database. The relevant information identification module 610 may cause the processor 602 to distinguish configuration information that is relevant to the standard from information that is not relevant to the standard.

[0042] The computer-readable medium 600 may include an information retrieval module 620 that causes the processor 602 to retrieve the identified configuration

information from the MDM database. For example, the information retrieval module 620 may cause the processor 602 to establish a direct, encrypted channel with the MDM database. Alternatively, or in addition, the information retrieval module 620 may cause the processor 602 to use an API of an MDM application to retrieve the identified configuration information (e.g., an API able to communicate the configuration information securely).

[0043] The computer-readable medium 600 may include a schema mapping module 630 that causes the processor 602 to map the identified configuration to a normalized schema to create normalized configuration information. The normalized schema may be a normalized schema that is readable by a compliance application and that allows the compliance application to determine conformity of the mobile device to the standard. For example, the configuration information may readily map to technical controls of the standard once the processor 602 has mapped it to the normalized schema. The computer-readable medium 600 may include an information storage module 640 that causes the processor 602 to store the normalized configuration information. For example, the information storage module 640 may cause the processor 602 to store the normalized configuration information in a persistent storage device. Referring to Figure 1, when executed by a processor, the relevant information identification module 610, the information retrieval module 620, the schema mapping module 630, and/or the information storage module 640 may realize a normalization component 120.

[0044] Figure 7 is a block diagram of an example of a computer-readable medium 700 containing instructions that, when executed by a processor 702, cause the processor 702 to map identifiers, configuration information, and detected vulnerabilities and threats to a schema readable by a compliance application. The computer-readable medium 700 may include a relevant information identification module 710 that causes the processor 702 to identify configuration information relevant to a standard governing IT assets. The computer-readable medium 700 may also include an information retrieval module 720 that causes the processor 702 to retrieve information, such as information relevant to the standard.

[0045] The information retrieval module 720 may include a configuration information retrieval module 722 and a vulnerability and threat retrieval module 724. The configuration information retrieval module 722 may cause the processor 702 to retrieve the configuration information from an MDM database and/or an MDM application. The vulnerability and threat retrieval module 724 may cause the processor 702 to receive indications of vulnerabilities and threats observed on the mobile device by a threat scanner (e.g., a threat seeking agent). In some examples, the vulnerability and threat retrieval module 724 may cause the processor 702 to receive the indications of vulnerabilities and threats from a threat scanner coordinator in communication with the threat scanner. The information retrieval module 720 may cause the processor to retrieve the configuration information and/or the indications of vulnerabilities and threats using a direct, mutually authenticated communication channel that is secure.

[0046] The computer-readable medium 700 may include a schema mapping module 730 that causes the processor 702 to map retrieved information to a normalized schema. The normalized schema may be readable by a compliance application to determine conformity of the mobile device to the standard. For example, the schema mapping module 730 may cause the processor to organize the retrieved information to correspond to technical controls of the standard as part of mapping the retrieved information to the normalized schema. The schema mapping module 730 may include a configuration information mapping module 734 that causes the processor 702 to map configuration information to the normalized schema and a vulnerability and threat mapping module 736 that causes the processor 702 to map indications of active vulnerabilities and threats to the normalized schema. Alternatively, the vulnerability and threat mapping module 736 may cause the processor 702 to map the indications of active vulnerabilities and threats to a normalized schema for active vulnerabilities and threats distinct from the normalized schema for configuration information.

[0047] The computer-readable medium 700 may include an identifier mapping module 732 to cause the processor 702 to map a unique identifier for the mobile device to an internet protocol (IP) address unused by other devices. For example, an MDM may use a unique identifier to reference the mobile device

(e.g., an international mobile equipment identity (IMEI), etc.), but a compliance application may use an IP address to uniquely reference each asset. Accordingly, the identifier mapping module 732 may cause the processor 702 to map the unique identifier used by the MDM to an IP address usable by the compliance application. The compliance application may not use the IP address to communicate with the mobile device, so the identifier mapping module 732 may cause the processor 702 to map the unique identifier used by the MDM to a dummy IP address that is not being used by fixed assets.

[0048] In an example, the identifier mapping module 732 may cause the processor 702 to map a set of mobile device identifiers to a set of IP address. The set of IP addresses may be a continuous range of addresses (e.g., a range of Class A IP addresses, a range of Class B IP addresses, a range of Class C IP addresses, etc.). Each IP address in the range may be unused, and there may be at least an IP address for each mobile identifier. The identifier mapping module 732 may cause the processor 702 to receive an indication of the range of unused of IP addresses (e.g., from a system administrator, from an application, etc.), to receive an indication of a range of IP addresses and indications of which IP addresses are used or unused, and/or the like.

[0049] For each mobile device identifier, the identifier mapping module 732 may cause the processor 702 to map the current mobile device identifier to a current IP address (e.g., starting from the first IP address in the range). The identifier mapping module 732 may cause the processor 702 to store an indication of the mapping, for example, in an associate array. The identifier mapping module 732 may cause the processor 702 to obtain the next mobile device identifier and increment to the next unused IP address in the range (e.g., increment by one if all addresses are unused). The identifier mapping module 732 may cause the processor 702 to continue mapping mobile device identifiers to available IP addresses until all mobile device identifiers have been mapped.

[0050] The computer-readable medium 700 may include an information storage module 740 that causes the processor 702 to store the mapped information (e.g., configuration information mapped to the normalized schema, indications of vulnerabilities and threats mapped to the normalized schema, indications of

mappings from mobile device identifiers to IP addresses, etc.). The information storage module 740 may cause the processor 702 to store the mapped information in a persistent storage device, in volatile memory, and/or the like. Alternatively, configuration information mapped to a first normalized schema may be stored separately from indications of vulnerabilities and threats mapped to a second normalized schema.

[0051] The computer-readable medium 700 may include a coordinator updating module 750 that causes the processor 702 to provide the stored information to the threat scanner and/or threat scanner coordinator so the threat scanner and/or threat scanner coordinator is aware of the state of the mobile device. The coordinator updating module 750 may cause the processor to provide the indication of the mapping of mobile device identifiers to IP addresses, the configuration information stored according to the normalized schema, etc. The threat scanner coordinator may not need to receive the indications of vulnerabilities and threats previously provided to the vulnerability and threat retrieval module 724 by the threat scanner coordinator. The coordinator updating module 750 may cause the processor 702 to provide the stored information periodically, aperiodically, on demand, or the like. Referring to Figure 1, when executed by a processor, the relevant information identification module 710, the information retrieval module 720, the schema mapping module 730, the information storage module 740, and/or the coordinator updating module 750 may realize a normalization component 120.

[0052] The above description is illustrative of various principles and implementations of the present disclosure. Numerous variations and modifications will become apparent to those skilled in the art once the above disclosure is fully appreciated. Accordingly, the scope of the present application should be determined only by the following claims.

CLAIMS

What is claimed is:

1. A system, comprising:

a normalization component to map configuration information for a mobile asset to a normalized schema to create normalized configuration information;

a compliance component to evaluate conformity of the mobile asset to a standard governing information technology assets based on the normalized configuration information.

2. The system of claim 1, wherein the compliance component is to:

identify vulnerabilities to the mobile asset based on the conformity of the mobile asset to the standard;

identify vulnerabilities to a fixed asset based on the standard;

evaluate the vulnerabilities to the mobile asset and the fixed asset under the standard; and

generate a report of risks to the mobile asset and the fixed asset based on the evaluating of the threats to the mobile asset and the fixed asset.

3. The system of claim 1, further comprising a coordination component to:

transmit threat descriptions to a threat seeking agent on the mobile asset;

receive an indication of an active threat observed by the threat seeking agent on the mobile asset; and

provide the indication of the active threat to a vulnerability normalization component,

wherein the vulnerability normalization component is to map the indication of the active threat to a schema for normalizing observed threats.

4. The system of claim 3, wherein the coordination component is to digitally sign the threat descriptions.

5. The system of claim 3, wherein the coordination component is to transmit, with the threat descriptions, a time when updated threat descriptions will be transmitted to the threat seeking agent on the mobile asset and a number monotonically increased with each transmission to the mobile asset.

6. The system of claim 3, wherein the coordination component is to transmit, with the threat descriptions, an indication of a priority for each threat description and a central processing unit usage goal.

7. A method, comprising:

selecting, using a processor, configuration information in a mobile device management database that corresponds to technical controls associated with a standard governing information technology assets;

evaluating, using the processor, the configuration information based on the technical controls to determine compliance of a mobile asset with the standard;

analyzing, using the processor, compliance of a fixed asset with the standard; and

generating, using the processor, a single report of risks for the mobile asset and the fixed asset.

8. The method of claim 7, further comprising:

determining a vulnerability of the mobile asset;

determining a set of notional commands to remediate the vulnerability;

translating the set of notional commands to actual commands for a mobile device management application for the mobile asset; and

communicating the actual commands to the mobile device management application, wherein communicating the actual commands includes digitally signing the actual commands.

9. The method of claim 8, further comprising:

receiving an indication from a ticketing system of an action to remediate the vulnerability,

wherein determining the set of notional commands comprises determining the set of notional commands to remediate the vulnerability based on the indication of the action to remediate the vulnerability.

10. The method of claim 9, further comprising:

receiving confirmation from the mobile device management application that the actual commands have been executed successfully; and

indicating to the ticketing system that the vulnerability has been remediated.

11. The method of claim 7, further comprising storing the configuration information in a predetermined structure, wherein evaluating the configuration information comprises retrieving the configuration information stored in the predetermined structure.

12. A non-transitory computer-readable medium comprising instructions that, when executed by a processor, cause the processor to:

identify configuration information for a mobile device relevant to a standard governing information technology assets, the configuration information stored in a mobile device management database;

retrieve the identified configuration information from the mobile device management database;

map the identified configuration information to a normalized schema for configuration information to create normalized configuration information, the normalized schema readable by a compliance application to determine conformity of the mobile device to the standard; and

store the normalized configuration information in a persistent storage device.

13. The computer-readable medium of claim 12, wherein the instructions, when executed by the processor, cause the processor to map a unique identifier for the mobile device to an internet protocol (IP) address unused by other devices.

14. The computer-readable medium of claim 12, wherein the instructions, when executed cause the processor to:

receive indications of vulnerabilities and threats observed on the mobile device by a threat scanner; and

store the indications of vulnerabilities and threats observed on the mobile device according to a normalized schema for vulnerabilities and threats.

15. The computer-readable medium of claim 14, wherein the instructions, when executed cause the processor to:

receive the indications of the vulnerabilities and threats from a threat scanner coordinator in communication with the threat scanner; and

provide the normalized configuration information to the threat scanner coordinator periodically.

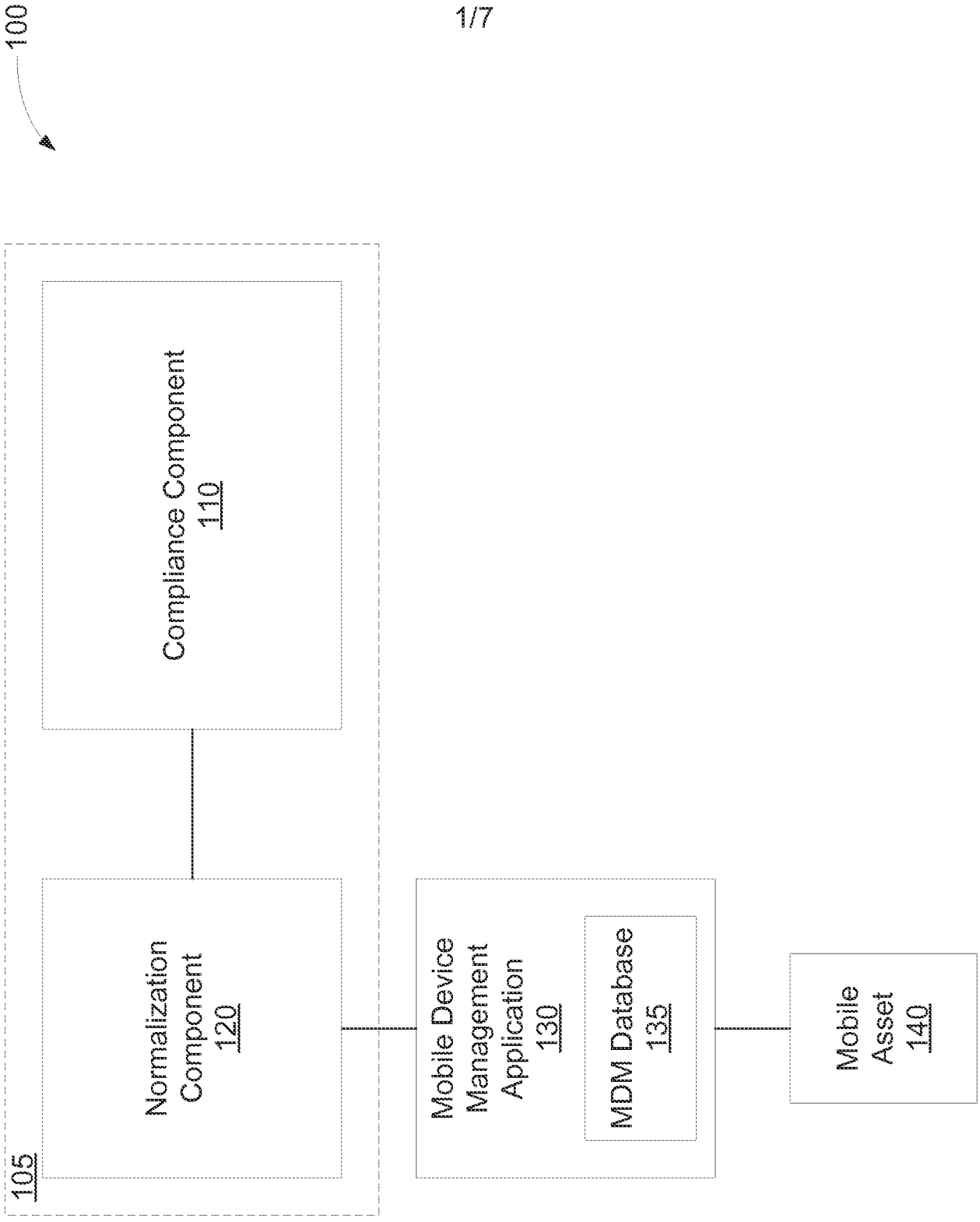

100
105
Compliance Component
110
Normalization
Component
120
Mobile Device
Management
Application
130
MDM Database
135
Mobile
Asset
140

FIG. 1

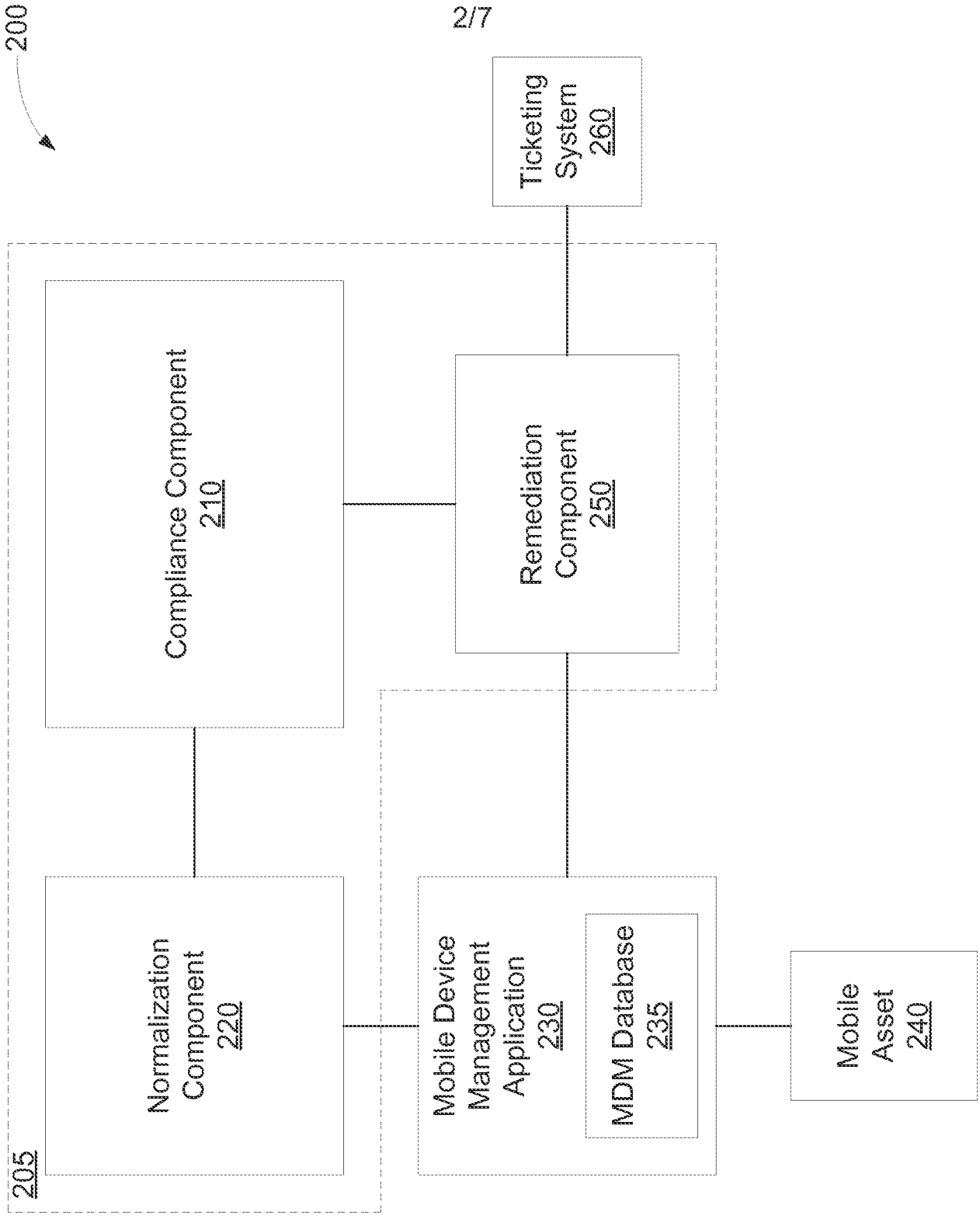

200
Ticketing System 260
Compliance Component 210
Remediation Component 250
Normalization Component 220
Mobile Device Management Application 230
MDM Database 235
Mobile Asset 240
205

FIG. 2

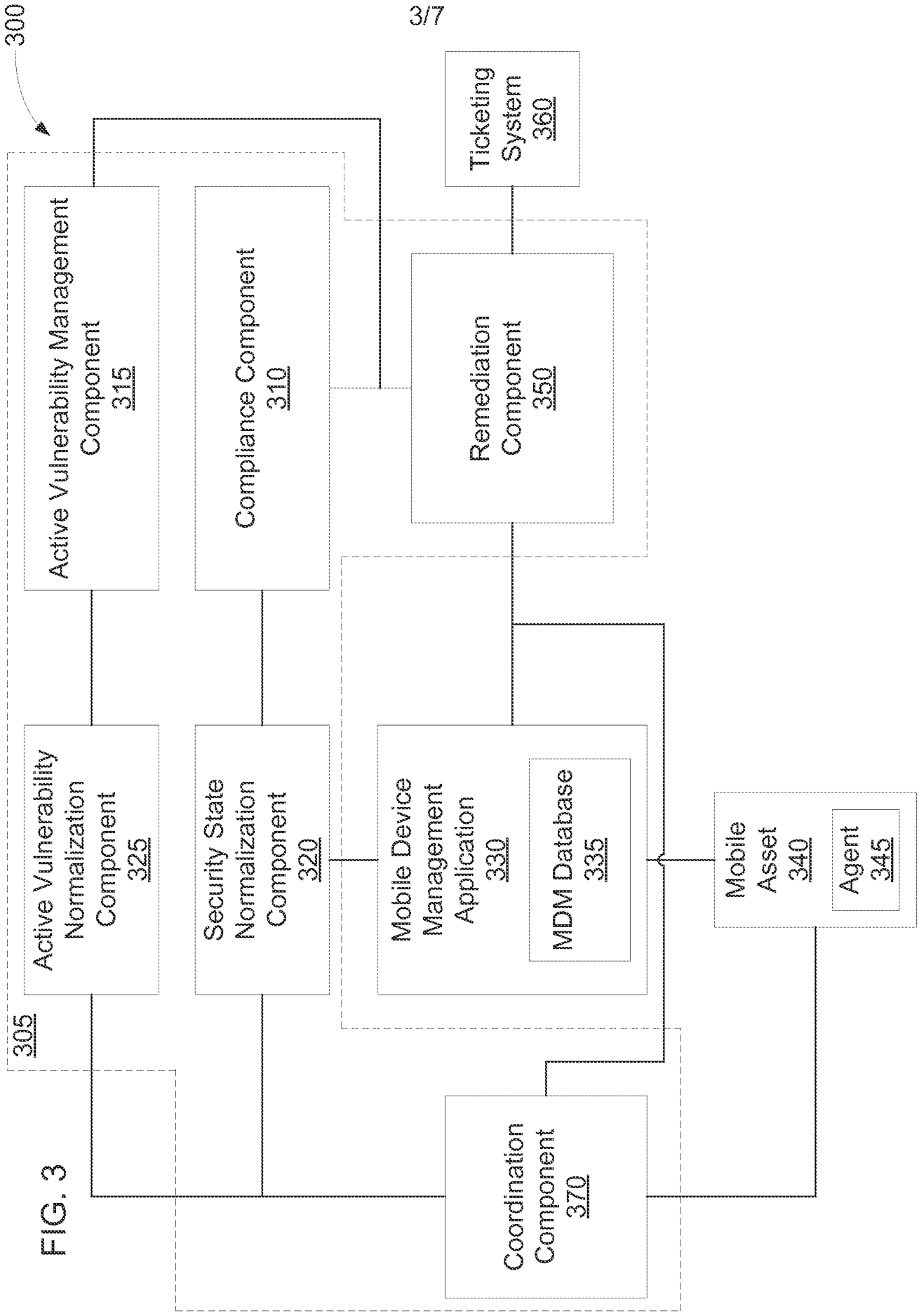

300
Ticketing System 360
Active Vulnerability Management Component 315
Compliance Component 310
Remediation Component 350
Active Vulnerability Normalization Component 325
Security State Normalization Component 320
Mobile Device Management Application 330
MDM Database 335
Mobile Asset 340
Agent 345
305
Coordination Component 370

FIG. 3

FIG. 4

400

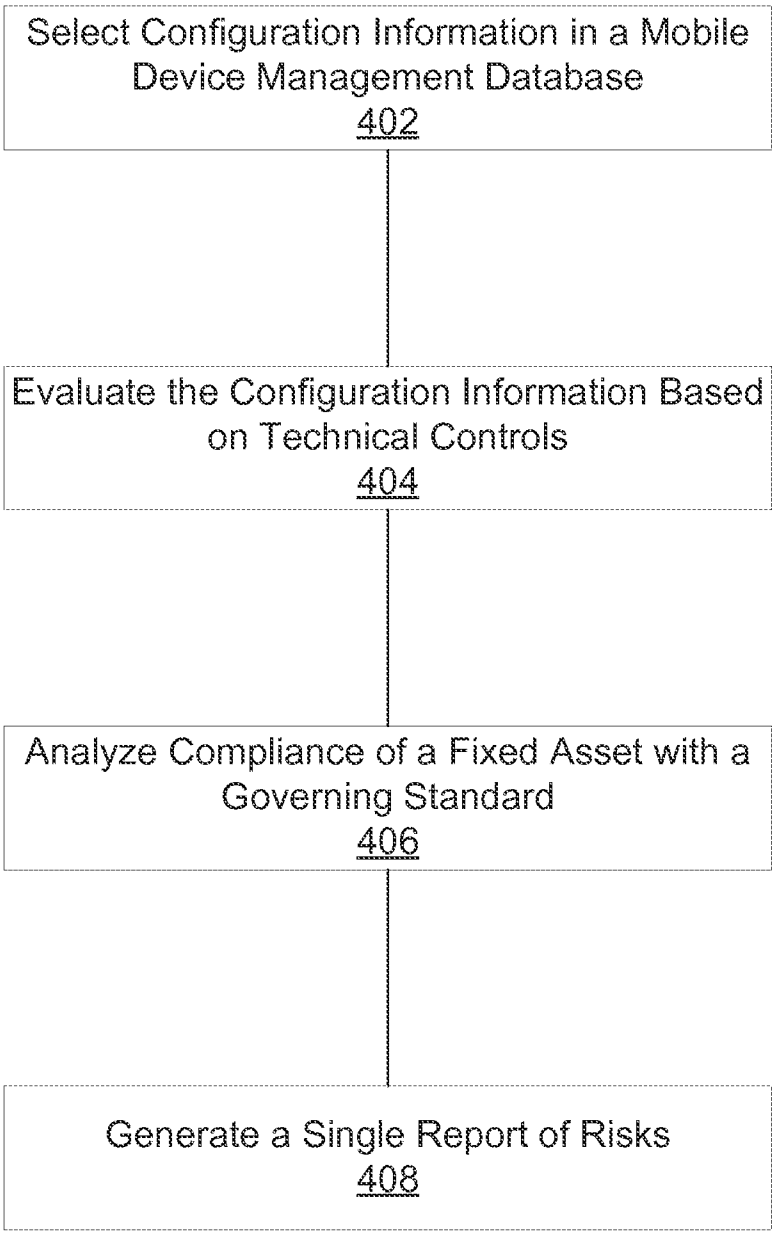

Select Configuration Information in a Mobile Device Management Database
402
Evaluate the Configuration Information Based on Technical Controls
404
Analyze Compliance of a Fixed Asset with a Governing Standard
406
Generate a Single Report of Risks
408

FIG. 5

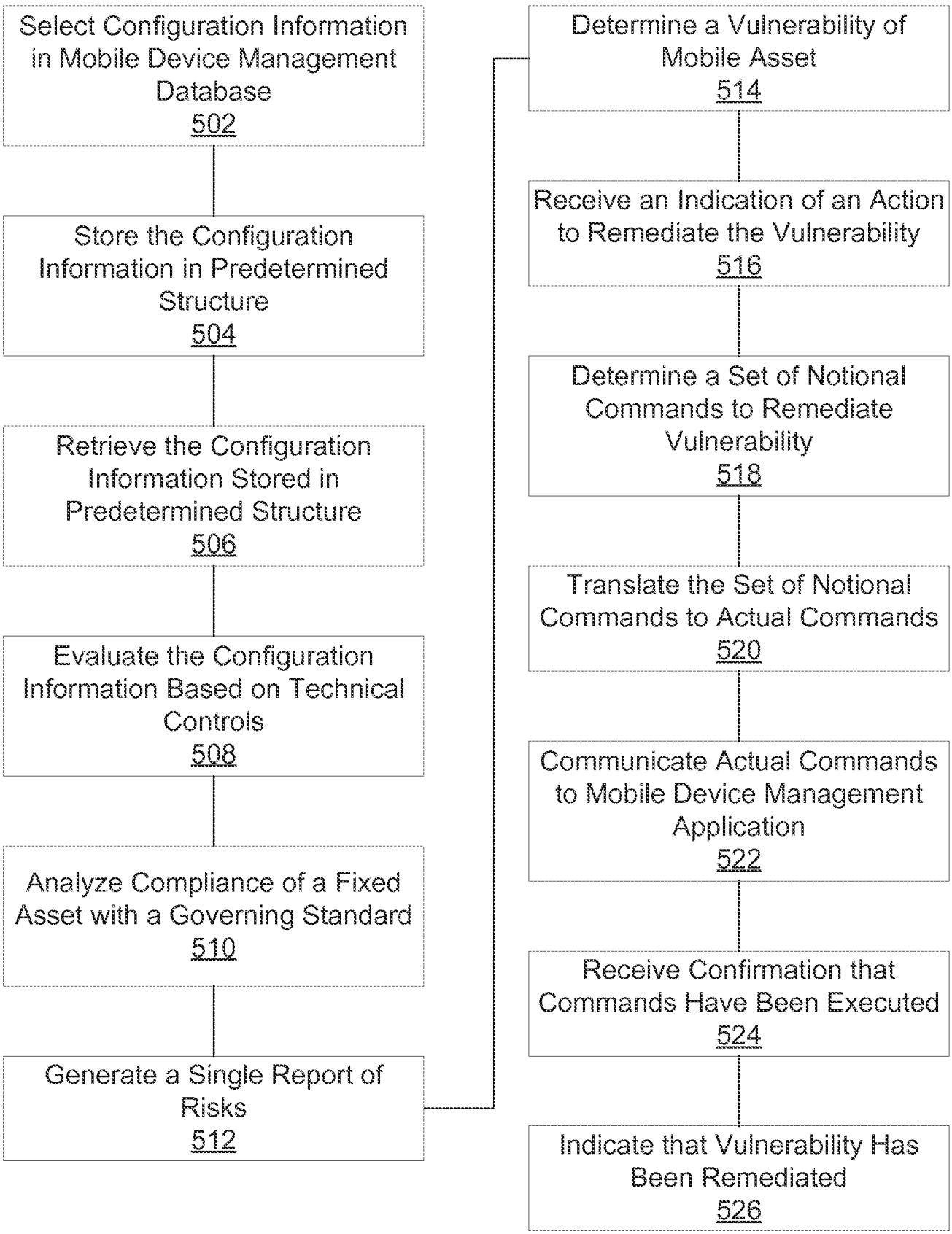

500
Select Configuration Information in Mobile Device Management Database
502
Store the Configuration Information in Predetermined Structure
504
Retrieve the Configuration Information Stored in Predetermined Structure
506
Evaluate the Configuration Information Based on Technical Controls
508
Analyze Compliance of a Fixed Asset with a Governing Standard
510
Generate a Single Report of Risks
512
Determine a Vulnerability of Mobile Asset
514
Receive an Indication of an Action to Remediate the Vulnerability
516
Determine a Set of Notional Commands to Remediate Vulnerability
518
Translate the Set of Notional Commands to Actual Commands
520
Communicate Actual Commands to Mobile Device Management Application
522
Receive Confirmation that Commands Have Been Executed
524
Indicate that Vulnerability Has Been Remediated
526

FIG. 6

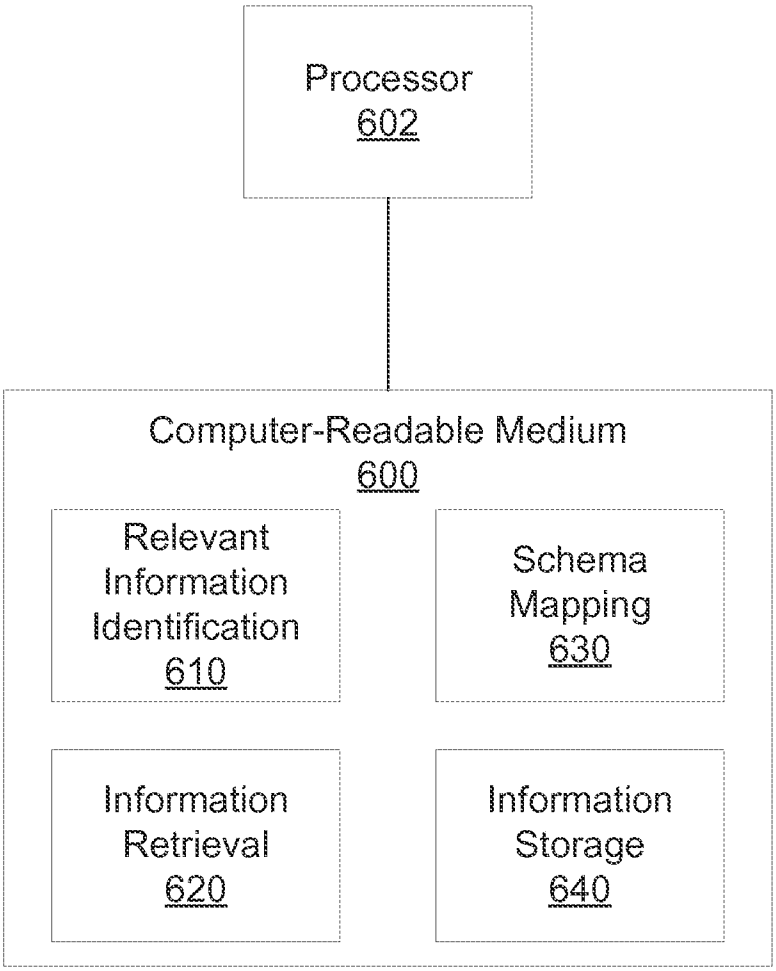
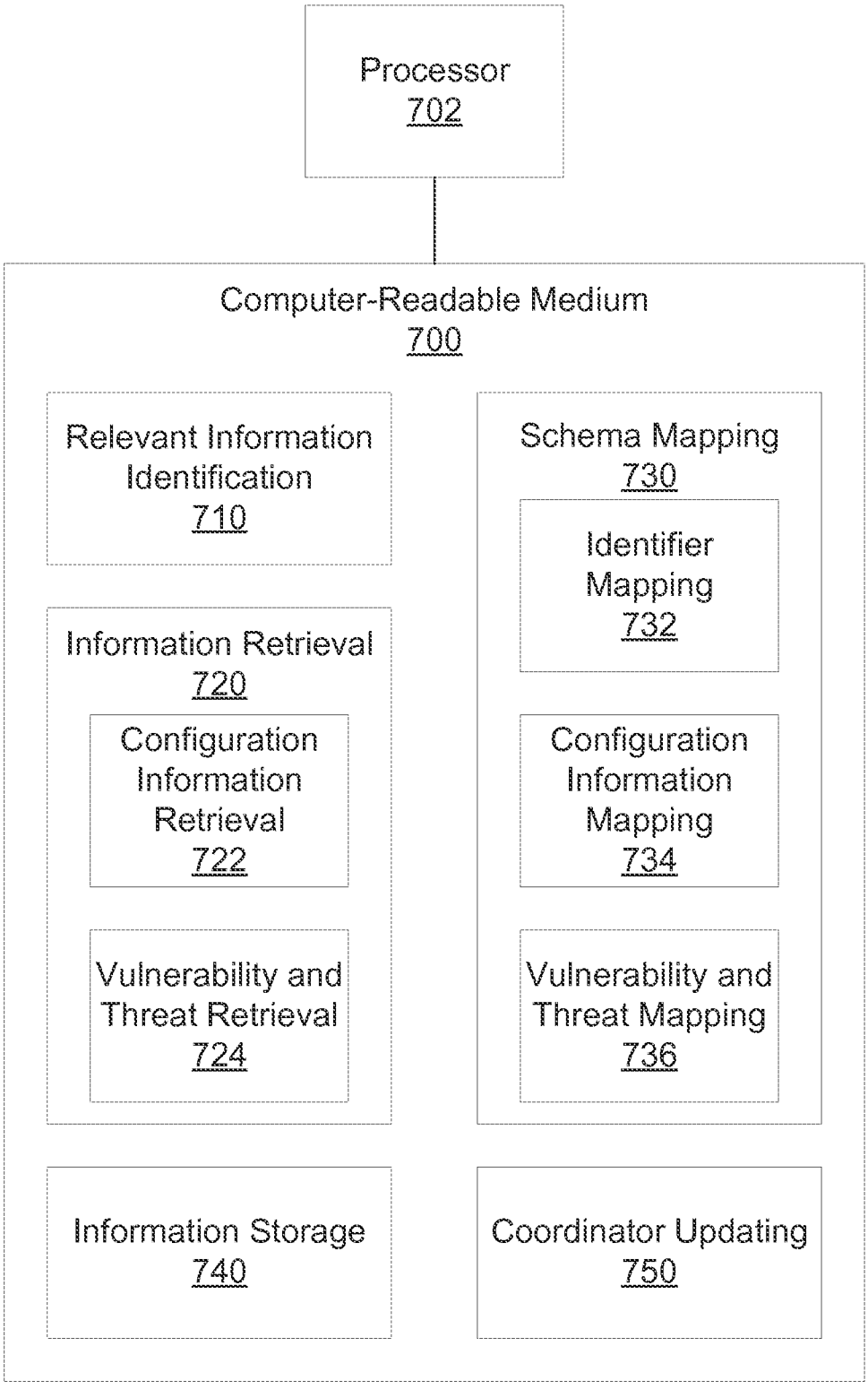

Processor
602
Computer-Readable Medium
600
Relevant Information Identification
610
Schema Mapping
630
Information Retrieval
620
Information Storage
640

FIG. 7


Processor
702
Computer-Readable Medium
700
Relevant Information Identification
710
Information Retrieval
720
Configuration Information Retrieval
722
Vulnerability and Threat Retrieval
724
Schema Mapping
730
Identifier Mapping
732
Configuration Information Mapping
734
Vulnerability and Threat Mapping
736
Information Storage
740
Coordinator Updating
750

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2015/031647

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 10/06(2012.01)i, G06Q 10/10(2012.01)i, G06Q 40/02(2012.01)i

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)
G06Q 10/06; G06F 15/16; G06F 17/30; G06F 21/57; H04L 29/06; G06F 21/00; G06Q 10/10; G06Q 40/02

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: mobile, asset, standard, compliance, configuration, mapping, normalized, schema, risk, report

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 8484694 B2 (SEBASTIEN DIEBLER et al.) 09 July 2013 See column 4, lines 3-5, column 5, lines 63-65, claims 1-3,10-12 and figures 1-2.	1-15
Y	US 8874685 B1 (ROBERT L. HOLLIS et al.) 28 October 2014 See column 4, lines 15-55, column 11, line 41 - column 12, line 2, column 14, line 45 - column 15, line 7 and figure 16.	1-6,10,12-15
Y	US 2013-0298230 A1 (SRINIVAS KUMAR et al.) 07 November 2013 See paragraphs [0104],[0200], claims 1,5-6 and figure 4.	2,7-11
A	US 2014-0156711 A1 (DHIRAJ SHARAN et al.) 05 June 2014 See abstract, paragraphs [0018]-[0019],[0022]-[0024],[0027], claims 1,15 and figure 1.	1-15
A	KR 10-2015-0040967 A (OPENPEAK INC.) 15 April 2015 See abstract, claims 1-10 and figure 2.	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 application or patent 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
29 February 2016 (29.02.2016)	**29 February 2016 (29.02.2016)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 35208,
Republic of Korea
Facsimile No. +82-42-472-7140

Authorized officer
Jang, Gijeong
Telephone No. +82-42-481-8364

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2015/031647

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 8484694 B2	09/07/2013	US 2010-0175106 A1	08/07/2010
		WO 2010-068824 A1	17/06/2010
US 8874685 B1	28/10/2014	None	
US 2013-0298230 A1	07/11/2013	JP 2015-519652 A	09/07/2015
		KR 10-2015-0006042 A	15/01/2015
		US 2013-0298192 A1	07/11/2013
		US 2013-0298242 A1	07/11/2013
		US 2013-0298243 A1	07/11/2013
		US 2013-0298244 A1	07/11/2013
		US 2015-0244735 A1	27/08/2015
		US 8776180 B2	08/07/2014
		US 8850588 B2	30/09/2014
		US 8990948 B2	24/03/2015
		US 9027125 B2	05/05/2015
		US 9092616 B2	28/07/2015
		WO 2013-166126 A1	07/11/2013
US 2014-0156711 A1	05/06/2014	CN 103827810 A	28/05/2014
		EP 2740028 A2	11/06/2014
		EP 2740028 A4	14/01/2015
		WO 2013-019879 A2	07/02/2013
		WO 2013-019879 A3	18/04/2013
KR 10-2015-0040967 A	15/04/2015	EP 2880583 A2	10/06/2015
		US 2012-0297444 A1	22/11/2012
		US 8713173 B2	29/04/2014
		WO 2014-077914 A2	22/05/2014
		WO 2014-077914 A3	21/08/2014