

User Interface For Security Protection And Remote Management Of Network Endpoints

RELATED APPLICATIONS

5 [0001] This application claims the benefit of the filing date of U.S. provisional patent applications No. 62/090,547, filed on Dec. 11, 2014, entitled "Systems and Methods for Securing Network Endpoints", No. 62/180,390, filed on Jun. 16, 2015, entitled "Systems and Methods for Automatic Device Detection, Device Management, and Remote Assistance", and No. 62/217,310, filed on Sep. 11, 2015, entitled "Systems and Methods for Automatic Network Service Takeover", the entire contents of which are incorporated by reference herein.

BACKGROUND

[0002] The invention relates to systems and methods for securing network endpoints against computer security threats, and to systems and methods for automatic device detection and remote device management.

15 [0003] Malicious software, also known as malware, affects a great number of computer systems worldwide. In its many forms such as computer viruses, exploits, and spyware, malware presents a serious risk to millions of computer users, making them vulnerable to loss of data and sensitive information, to identity theft, and to loss of productivity, among others.

20 [0004] A great variety of devices, informally referred to as the Internet of Things (IoT), are currently being connected to communication networks and the Internet. Such devices include, among others, smartphones, smartwatches, TVs and other multimedia devices, game consoles, home appliances, and various home sensors such as thermostats. As more such devices go online, they become targets for security threats. Therefore, there is an increasing need of securing such devices against malware, as well as of protecting communications to and from such devices.

25 [0005] In addition, the proliferation of such intelligent devices in environments such as homes and offices creates an increasing problem of device and network management. When each device uses a distinct configuration interface and requires separate connection settings, managing a large number of such devices may become a burden, especially for a typical home user who is

not experienced in network administration. Therefore, there is an increasing interest in developing systems and methods for automatic device detection and configuration, with particular emphasis on security.

SUMMARY

5 **[0006]** According to one aspect, a computing system comprises a hardware processor and a memory, the memory storing instructions which, when executed by the hardware processor, cause the computing system to receive data from a remote server, the data selected by the server for transmission to the computing system according to a subscription associated with a network regulator protecting a plurality of client systems against computer security threats, wherein the
10 plurality of client systems are connected to the network regulator over a local network. The instructions further cause the computing system to perform a display of a graphical user interface (GUI) configured to generate a device management view enabling a user to remotely configure a client system of the plurality of client systems, and to generate a security notification view displaying an indicator of a security event caused by an action of the client system. The network
15 regulator is configured, in response to connecting to a router providing a network service to the plurality of client systems, to automatically take over the network service from the router, wherein the network service comprises supplying network addresses to the plurality of client systems.

20 **[0007]** According to another aspect, a method comprises employing a network regulator to protect a plurality of client systems against computer security threats, wherein the plurality of client systems are connected to the network regulator over a local network. The method further comprises employing the network regulator, in response to connecting to a router providing a network service to the plurality of client systems, to automatically take over the network service from the router, wherein the network service comprises supplying network addresses to the
25 plurality of client systems. The method further comprises, in response to the network regulator taking over the network service, employing a hardware processor of a computing system to receive data from a remote server, the data selected by the server for transmission to the computing system according to a subscription associated with the network regulator. The method further comprises, in response to the network regulator taking over the network service,
30 employing the hardware processor to perform a display of a graphical user interface (GUI). The

GUI is configured to generate a device management view enabling a user to remotely configure a client system of the plurality of client systems, and further configured to generate a security notification view displaying an indicator of a security event caused by an action of the client system.

5 [0008] According to another aspect, a non-transitory computer-readable medium stores instructions which, when executed by a hardware processor of a computing system, cause the computing system to receive data from a remote server, the data selected by the server for transmission to the computing system according to a subscription associated with a network regulator protecting a plurality of client systems against computer security threats, wherein the
10 plurality of client systems are connected to the network regulator over a local network. The instructions further cause the computing system to perform a display of a graphical user interface (GUI). The GUI is configured to generate a device management view enabling a user to remotely configure a client system of the plurality of client systems, and further configured to generate a security notification view displaying an indicator of a security event caused by an
15 action of the client system. The network regulator is configured, in response to connecting to a router providing a network service to the plurality of client systems, to automatically take over the network service from the router, wherein the network service comprises supplying network addresses to the plurality of client systems.

BRIEF DESCRIPTION OF THE DRAWINGS

20 [0009] The foregoing aspects and advantages of the present invention will become better understood upon reading the following detailed description and upon reference to the drawings where:

[0010] Fig. 1-A shows an exemplary configuration of client systems interconnected by a local network, and a network regulator protecting the client systems against computers security threats
25 according to some embodiments of the present invention.

[0011] Fig. 1-B shows alternative configuration of client systems and network regulator according to some embodiments of the present invention.

[0012] Fig. 2 illustrates an exemplary hardware configuration of a client system according to some embodiments of the present invention.

[0013] Fig. 3 illustrates an exemplary hardware configuration of a network regulator according to some embodiments of the present invention.

5 [0014] Fig. 4 illustrates an exemplary hardware configuration of an administration device according to some embodiments of the present invention.

[0015] Fig. 5 shows a set of remote servers collaborating with the network regulator to protect client systems from computer security threats, according to some embodiments of the present invention.

10 [0016] Fig. 6-A illustrates an embodiment of the present invention, wherein a part of a network traffic is scanned at the security server according to some embodiments of the present invention.

[0017] Fig. 6-B shows an embodiment of the present invention, wherein a part of a network traffic is scanned by the network regulator according to some embodiments of the present invention.

15 [0018] Fig. 7 shows an exemplary sequence of steps performed by the network regulator according to some embodiments of the present invention.

[0019] Fig. 8 shows exemplary software components executing on the administration device according to some embodiments of the present invention.

20 [0020] Fig. 9 shows an exemplary data exchange between a client system, the network regulator, the client configuration server, and the administration device according to some embodiments of the present invention, the data exchange occurring as part of configuring the respective client system.

25 [0021] Fig. 10 illustrates an exemplary sequence of steps performed by the administration device and/or client configuration server to configure a client system according to some embodiments of the present invention.

[0022] Fig. 11 shows an exemplary data exchange between a client system, the network regulator, the security server, and the administration device according to some embodiments of the present invention, the data exchange occurring as part of event notification.

5 [0023] Fig. 12 illustrates an exemplary sequence of steps performed by the administration device and/or security server to notify a user about the occurrence of an event involving a protected client system, according to some embodiments of the present invention.

[0024] Fig. 13-A shows an exemplary sequence of steps performed by the administration device to operate a client configuration graphical user interface (GUI) according to some embodiments of the present invention.

10 [0025] Fig. 13-B shows further exemplary steps performed by the administration device to operate the client configuration GUI according to some embodiments of the present invention.

[0026] Fig. 14 shows an exemplary sequence of steps performed by the administration device to operate a notification GUI according to some embodiments of the present invention.

15 [0027] Fig. 15 shows an exemplary device management view generated by an administration GUI executing on the administration device according to some embodiments of the present invention. The view illustrates exemplary configurable parameters of the network regulator.

[0028] Fig. 16 shows another exemplary device management view according to some embodiments of the present invention. The view illustrates exemplary data displayed during the initial setup of a client system.

20 [0029] Fig. 17-A shows another exemplary device management view of the GUI, the view illustrating various device configuration options according to some embodiments of the present invention.

[0030] Fig. 17-B shows yet another exemplary device management view illustrating other device configuration options according to some embodiments of the present invention.

[0031] Fig. 18 shows an exemplary device management view enabling a user to associate an owner with the client system currently undergoing configuration, according to some embodiments of the present invention.

5 [0032] Fig. 19 shows an exemplary device management view illustrating a current state of a configured client system according to some embodiments of the present invention.

[0033] Fig. 20-A illustrates an exemplary device management view displaying vulnerability assessment information for a protected client system, according to some embodiments of the present invention.

10 [0034] Fig. 20-B shows an exemplary device management view displaying further vulnerability information according to some embodiments of the present invention.

[0035] Fig. 21 shows yet another exemplary device management view generated by the administration GUI, the view displaying a list of protected devices according to some embodiments of the present invention.

15 [0036] Fig. 22-A illustrates an exemplary notification view generated by the GUI, the view displaying a first part of a list of event notifications according to some embodiments of the present invention.

[0037] Fig. 22-B shows a second part of the list of event notifications according to some embodiments of the present invention.

20 [0038] Fig. 23 shows an exemplary notification view displaying details of a security event according to some embodiments of the present invention.

[0039] Fig. 24-A shows another exemplary notification view displaying a device maintenance event according to some embodiments of the present invention.

25 [0040] Fig. 24-B shows yet another exemplary notification view generated by the administration GUI, the view displaying another device maintenance event according to some embodiments of the present invention.

DETAILED DESCRIPTION

[0041] In the following description, it is understood that all recited connections between structures can be direct operative connections or indirect operative connections through intermediary structures. A set of elements includes one or more elements. Any recitation of an element is understood to refer to at least one element. A plurality of elements includes at least two elements. Unless otherwise required, any described method steps need not be necessarily performed in a particular illustrated order. A first element (e.g. data) derived from a second element encompasses a first element equal to the second element, as well as a first element generated by processing the second element and optionally other data. Making a determination or decision according to a parameter encompasses making the determination or decision according to the parameter and optionally according to other data. Unless otherwise specified, an indicator of some quantity/data may be the quantity/data itself, or an indicator different from the quantity/data itself. Computer security encompasses protecting users and equipment against unintended or unauthorized access to data and/or hardware, against unintended or unauthorized modification of data and/or hardware, and against destruction of data and/or hardware. A computer program is a sequence of processor instructions carrying out a task. Computer programs described in some embodiments of the present invention may be stand-alone software entities or sub-entities (e.g., subroutines, libraries) of other computer programs. Two devices are said to be connected to or to belong to the same local network when their network addresses belong to the same subnet and/or when both have the same broadcast address. A tunnel is a virtual point-to-point connection between two entities connected to a communication network. Computer readable media encompass non-transitory media such as magnetic, optic, and semiconductor storage media (e.g. hard drives, optical disks, flash memory, DRAM), as well as communication links such as conductive cables and fiber optic links. According to some embodiments, the present invention provides, *inter alia*, computer systems comprising hardware (e.g. one or more microprocessors) programmed to perform the methods described herein, as well as computer-readable media encoding instructions to perform the methods described herein.

[0042] Figs. 1-A-B show exemplary network configurations 10a-b according to some embodiments of the present invention, wherein a plurality of client systems 12a-f are interconnected by way of a local network 14, and further connected to an extended network 16,

such as the Internet. Client systems **12a-f** may represent any electronic device having a processor, a memory, and a communication interface. Exemplary client systems **12a-f** include personal computers, laptops, tablet computers, mobile telecommunication devices (e.g., smartphones), media players, TVs, game consoles, home appliances (e.g., refrigerators, thermostats, intelligent heating and/or lighting systems), and wearable devices (e.g., smartwatches, sports and fitness equipment), among others. Local network **14** may comprise a local area network (LAN). Exemplary local networks **14** may include a home network and a corporate network, among others.

[0043] Router **19** comprises an electronic device enabling communication between client systems **12a-f** and/or access of client systems **12a-f** to extended network **16**. In some embodiments, router **19** acts as a gateway between local network **14** and extended network **16**, and provides a set of network services to client systems **12a-f**. Unless otherwise specified, the term network services is used herein to denote services enabling the inter-communication of client systems **12a-f**, as well as communication between client systems **12a-f** and other entities. Such services may include, for instance, distributing network configuration parameters (e.g., network addresses) to clients systems **12a-f**, and routing communication between participating endpoints. Exemplary network services implement a dynamic host configuration protocol (DHCP).

[0044] Figs. **1-A-B** further show a network regulator **18** connected to local network **14**. In some embodiments, network regulator **18** comprises a network appliance configured to perform various services for client systems **12a-f**. Such services include, among others, computer security services (e.g., anti-malware, intrusion detection, anti-spyware, etc.), device management (e.g., remote configuration of client systems **12a-f**), parental control services, secure communication services (e.g., virtual private networking – VPN), and remote technical assistance (e.g., device and/or network troubleshooting).

[0045] In a typical application according to some embodiments of the present invention, network regulator **18** is introduced to a local network already configured and managed by router **19**. In some embodiments, at installation, regulator **18** takes over network services such as DHCP from router **19** and installs itself in a gateway position between local network **14** and extended

network **16**, so that at least a part of the traffic between client systems **12a-f** and extended network **16** traverses network regulator **18** (see Fig. 1-A). Placing network regulator **18** in a gateway position may be preferable because, in some embodiments, regulator **18** provides computer security services by redirecting at least some of the traffic (e.g., HTTP requests) from client systems **12a-f** to a security server. Having regulator **18** in a gateway position may facilitate the interception of such traffic.

[0046] In some embodiments such as the example in Fig. 1-B, router **19** may continue to operate as gateway for local network **14** after installation of regulator **18**, but in such cases network regulator **18** is preferably positioned between client systems **12a-f** and the existing gateway (i.e., router **19**), so that regulator **18** belongs to the same local network as client systems **12a-f**. Such a position is preferred because, in some embodiments, network regulator **18** is configured to collaborate with a remote server to detect the type of each client system (e.g., smartphone vs. PC), and in response, to deliver a device-specific utility agent to some of client systems **12a-f**. Configurations wherein regulator **18** is not a member of local network **14** (e.g., placing regulator **18** between router **19** and extended network **16**) may make such device discovery and agent delivery more difficult.

[0047] In some embodiments, client systems **12a-f** are monitored, managed, and/or configured remotely by a user/administrator, using software executing on an administration device **20** connected to extended network **16** (e.g., the Internet). Exemplary administration devices **20** include smartphones and personal computer systems, among others. Device **20** may expose a graphical user interface (GUI) allowing a user to remotely configure and/or manage operation of client systems **12a-f**, for instance to set configuration options and/or to receive notifications about security-related events occurring on the respective client systems.

[0048] Figs. 2-3-4 show exemplary hardware configurations of a client system **12**, network regulator **18**, and administration device **20**, respectively. Without loss of generality, the illustrated configurations correspond to computer systems (Fig. 2-3) and a smartphone (Fig. 4). The hardware configuration of other systems (e.g., tablet computers) may differ from the ones illustrated in Figs. 2-3-4. In some embodiments, each of processors **22**, **122**, and **222** comprises a physical device (e.g. microprocessor, multi-core integrated circuit formed on a semiconductor

substrate) configured to execute computational and/or logical operations with a set of signals and/or data. Memory units unit **24**, **124**, and **224** may comprise volatile computer-readable media (e.g. RAM) storing data/signals accessed or generated by processors **22**, **122**, and **222**, respectively, in the course of carrying out operations.

5 **[0049]** Input devices **26**, **226** may include computer keyboards, mice, and microphones, among others, including the respective hardware interfaces and/or adapters allowing a user to introduce data and/or instructions into the respective system. Output devices **28**, **228** may include display devices such as monitors and speakers among others, as well as hardware interfaces/adapters such as graphic cards, allowing the respective system to communicate data to a user. In some
10 embodiments, input and output devices share a common piece of hardware (e.g., touch-screen). Storage devices **32**, **132**, and **232** include computer-readable media enabling the non-volatile storage, reading, and writing of software instructions and/or data. Exemplary storage devices include magnetic and optical disks and flash memory devices, as well as removable media such as CD and/or DVD disks and drives.

15 **[0050]** Network adapters **34**, **134** enable client system **12** and network regulator **18**, respectively, to connect to an electronic communication network such as local network **14**, and/or to other devices/computer systems. Communication devices **40** (Fig. 4) enable administration device **20** to connect to extended network **16** (e.g., the Internet), and may include telecommunication hardware (electromagnetic wave emitters/receivers, antenna, etc.). Depending on device type
20 and configuration, administration device **20** may further include a geolocation device **42** (e.g. GPS receiver), and a set of sensing devices **136** (e.g., motion sensors, light sensors, etc.).

[0051] Controller hubs **30**, **130**, **230** represent the plurality of system, peripheral, and/or chipset buses, and/or all other circuitry enabling the communication between the processor of each respective system and the rest of the hardware components. In an exemplary client system **12**
25 (Fig. 2), hub **30** may comprise a memory controller, an input/output (I/O) controller, and an interrupt controller. Depending on hardware manufacturer, some such controllers may be incorporated into a single integrated circuit, and/or may be integrated with the processor.

[0052] In some embodiments, network regulator **18** further comprises a protected storage module **38**. Module **38** may comprise a hardware device (for instance a persistent memory

circuit) configured to securely store sensitive information. Module **38** may be configured so that software executing on the network regulator may not overwrite a content of module **38**. The secure storage may be used to store a cryptographic key uniquely associated with the respective network regulator (such keys are known as endorsement keys in some embodiments). In some
5 embodiments, protected storage module **38** also comprises a cryptographic processor configured to generate cryptographic keys, to compute hashes, and/or to perform encryption/decryption of data. Exemplary protected storage modules **38** include trusted platform module (TPM) chips produced by various hardware manufacturers. In an alternative embodiment, protected storage module **36** may be software-emulated, for instance using ARM TrustZone® technology.

10 **[0053]** In some embodiments, network regulator **18** comprises an identification token, which may be used to uniquely identify the respective network regulator from among a plurality of similar devices. Each identification token may be associated with a subscription or service account. In some embodiments, the identification token is stored in protected storage module **38** of regulator **18**.

15 **[0054]** In some embodiments, network regulator **18** may collaborate with a set of remote computer systems to protect client systems **12a-f** from computer security threats. Such threats include, among others, malicious software (e.g., viruses, Trojans, spyware), network intrusion by unauthorized third parties, data theft, traffic surveillance, and electronic fraud. Exemplary remote computer systems include a security server **50** and a client configuration server **52**,
20 illustrated in Fig. 5. Servers **50** and **52** may comprise individual machines, or clusters of multiple interconnected computer systems. In some embodiments, security server **50** performs threat detection operations (e.g., malware detection, intrusion prevention, etc.), to detect security events involving a protected client system, such as client systems **12a-f** in Figs. 1-A-B. Security server **50** may be further connected to an event database comprising a plurality of security
25 records, each security record including data indicative of a security event, as well as an indicator of an association between the respective event and a protected client system **12**.

[0055] In some embodiments, configuration server **52** collaborates with administration device **20** to configure device management and/or security settings of regulator **18**, router **19**, and/or of a protected client system **12**. Server **52** may be communicatively connected to a subscriber

database **54** and to a device feature database **56**. Subscriber database **54** may store a plurality of subscription records, each subscription record indicative of a set of client systems under device management according to some embodiments of the present invention. In one embodiment, each subscription record is uniquely associated with a distinct network regulator **18**. In such
5 embodiments, all client systems **12** configured and/or otherwise serviced using the respective network regulator (e.g., client systems **12a-f** connected to local network **14** in Fig. **1-A**) are associated with the same subscription record. Each subscription record may include an indicator of a subscription period and/or a set of subscription parameters describing, for instance, a desired level of security or a selection of services subscribed for. Subscriptions may be managed
10 according to a service-level agreement (SLA).

[0056] In some embodiments, device feature database **56** comprises a set of records indicating configurable features of each client system **12** and/or current configuration settings for each client system. Database **56** may further comprise a comprehensive set of records usable to determine a device type of client system **12**. Such records may include entries corresponding to
15 various device types (e.g., routers, smartphones, wearable devices, etc.), makes, and models, from various manufacturers, using various operating systems (e.g., Windows® vs. Linux®). An exemplary entry may comprise, among others, indicators of whether the respective device type uses a particular network protocol to communicate (e.g., HTTP, Bonjour®), an indicator of a layout of a login interface exposed by the respective device type, etc.

[0057] Figs. **6-A-B** show exemplary embodiments wherein network regulator **18** collaborates with security server **50** to protect client systems **12a-f** from computer security threats such as malware, adware, spyware, and network intrusion. In the embodiment of Fig. **6-A**, network regulator **18** re-routes some or all of the data traffic (herein illustrated by network packet **60**) between protected client system **12** and a computer system external to the local network through
20 security server **50**. Such re-routing may be achieved, for instance, by installing network regulator **18** as gateway between local network **14** and extended network **16**, and using regulator **18** to intercept network traffic and actively redirect it to server **50**. In embodiments as illustrated in Fig. **6-A**, threat detection is performed by security server **50**, using any method known in the art (e.g., by analyzing network packets **60** to determine whether they contain
25 malware, or whether they are indicative of a network intrusion).

[0058] In some embodiments, as illustrated in Fig. 6-B, threat detection is performed by network regulator 18. Such local detection may comprise, for instance, filtering packet content. Regulator 18 may keep malware detection algorithms up to date by downloading a set of filter parameters 62 (e.g. malware-indicative signatures) from security server 50. Some embodiments
5 may combine threat detection on regulator 18 with threat detection at security server 50. In one such example, network regulator 18 may carry out a preliminary analysis of data traffic, using, for instance, relatively inexpensive methods. Regulator 18 may then send suspect network packets for further analysis to server 50.

[0059] Re-routing traffic through security server 50 (Fig. 6-A) may have several advantages over
10 performing a local security analysis (Fig. 6-B). Server 50 may comprise multiple purpose-built, high-throughput computer systems, and may therefore be able to carry out computationally intensive traffic analysis, such as deep packet inspection, much more efficiently than regulator 18. Installing such capabilities in network regulator 18 would substantially increase the price, complexity, and attack surface of regulator 18. Another advantage of having centralized
15 data analysis is that such configurations eliminate the need to distribute updates of malware-identifying signatures and of other data used in network packet analysis to a large number of distributed network regulators 18. Centralized security systems are also typically better equipped to respond to newly discovered threats.

[0060] An exemplary application of such computer security systems and methods comprises
20 blocking access of a protected client system to malicious or fraudulent webpages. In one such example, a request to access a remote resource (e.g., a HTTP request from a protected client system) is intercepted and analyzed to determine whether access to the remote resource, webpage, etc., represents a computer security risk. Such analysis may use any method known in the art, for instance matching an address of the respective resource against a blacklist of known
25 malicious or fraudulent webpages, analyzing the layout of the respective webpage, etc. The analysis may be carried out at security server 50 (e.g., in a configuration as shown in Fig. 6-A) or at network regulator 18 (e.g., as shown in Fig. 6-B). When the analysis establishes that accessing the remote resource does not amount to a computer security risk, the respective client system is allowed access to the respective remote resource. When access is deemed risky, the
30 requesting client system may be blocked from accessing the respective resource. In addition to

blocking access, some embodiments of security server **50** send an event notification to administration device **20**, informing the user/administrator of network regulator **18** that a security event has occurred. The notification may include an indicator of the client system involved in the respective event, and an indicator of a type of event (e.g., access to a fraudulent website).

5 **[0061]** Fig 7 shows a sequence of steps executed by network regulator **18** according to some embodiments of the present invention. Such a sequence may be executed, for instance, upon installation of network regulator **18**, or when regulator **18** is first introduced to local network **14**. In a step **300**, regulator **18** automatically detects router **19**, herein representing the existing provider of network services. In some embodiments, regulator **18** then takes over some of the
10 network services from router **19**. Such takeover may comprise shutting off or otherwise incapacitating some of the functionality of router **19** (e.g. a Dynamic Host Configuration Protocol – DHCP – server of router **19**), and replacing router **19** as the provider of at least a part of the network services associated with local network **14**. In an alternative embodiment, service takeover may comprise offering an alternative set of network services in addition to those
15 managed by router **19**, without actually incapacitating the latter. In some embodiments, step **302** further comprises installing network regulator **18** in a gateway position between local network **14** and extended network **16**, so that at least a part of network traffic between client systems **12a-f** and extended network **16** traverses regulator **18**.

20 **[0062]** In a sequence of steps **304-306**, network regulator **18** may automatically detect devices belonging to local network **14** (i.e., client systems **12a-f**), and distribute device-specific utility agents **41** to at least some of client systems **12a-f**. A broad variety of utility agents may be provisioned using systems and methods described herein. Examples include computer security agents, parental control agents, and remote technical assistance agents, among others. A further step **308** performs a set of computer security services for client systems **12a-f**.

25 **[0063]** Fig. 8 shows an exemplary set of software components executing on administration device **20** (e.g., a smartphone), according to some embodiments of the present invention. Such software components may include an operating system **63** and a set of applications. Applications include an administration application **64** configured to enable a user to remotely configure protection of client systems **12a-f**. Configuring protection of systems **12a-f** may include, among

others, configuring client-specific security settings, configuring client-specific network access parameters (e.g., connection speed, etc.), and launching maintenance tasks (e.g., software upgrades, disk cleanup operations, etc.). Administration application **64** may expose an administration graphical user interface (GUI) **65** to a user of administration device **20**. The operation of GUI **65** is further illustrated below.

[0064] Figs. 9-10 show an exemplary data exchange and a sequence of steps, respectively, occurring as part of remotely configuring protection of client system **12**. Such exchanges may occur during the initial configuration of client system **12**, or for subsequent parameter changes. Client system **12** may be configured remotely by an administrator via administration GUI **65** exposed on administration device **20**. For this purpose, GUI **65** may generate a device management view displaying a plurality of configurable parameters used by client system **12** and/or by network regulator **18** to protect the respective client system. The device management view further enables the administrator to select desired values for such parameters. In some embodiments, configurable parameters may be device-specific, for instance, may vary between a computer system and a smartphone. Also, configurable parameters may differ between devices running different operating systems (e.g., Windows® vs. iOS® or Android). In some embodiments, server **52** maintains a database of device-specific configuration parameters (e.g., device feature database **56**, Fig. 5) and a database of current parameter values for each protected client system **12** (e.g., subscriber database **54**).

[0065] In some embodiments, device **20** obtains a list of current configurable parameter and/or parameters values (e.g., current configuration settings **77** in Fig. 9) from configuration server **52**. To selectively retrieve client-specific configuration parameters and/or parameter values from databases **54-56**, some embodiments of server **52** use a client ID **78** received from administration device **20** as a lookup key. Client ID **78** may uniquely identify each protected client system, and may also include an identifying token of network regulator **18** controlling the local network to which the respective client system is currently connected. The client ID may be obtained by server **52** and/or administration device **20** during device discovery of client system **12**.

[0066] In response to the administrator's entering changes to the configuration parameters into administration GUI **65**, a set of updated configuration settings **80** is sent from administration

device 20 to server 52, which may forward updated settings 80 to network regulator 18 and/or to the respective client system 12. Some such settings may configure network regulator 18 (e.g. to set a limit on the connection speed and/or on the amount of data transferred to/from the respective client system). Other settings may configure client system 12 directly (e.g., to order a software update, to set a thermostat to a new temperature, etc.).

[0067] In some embodiments, a client management agent executing on client system 12 may perform a security assessment of client system 12 and may send assessment data to client configuration server 52 or security server 50. The server(s) may then forward client security assessment 81 to administration device 20 for display to the administrator. An exemplary security assessment 81 may include, among others, an indicator of whether a particular software object executing on client system 12 is up to date, and an indicator of a quality of a password used to protect client system 12.

[0068] In some embodiments, GUI 65 may further generate a notification view displaying a set of notifications, each such notification communicating to the administrator the occurrence and details of an event. The event may be a security event (e.g., a blocked phishing attempt), a device management event (e.g., a software update, an arming or disarming of a home security system), etc. Fig. 11 shows an exemplary data exchange occurring during event notification. In some embodiments, the event is detected either by security server 50 or by network regulator 18. When the event was detected at network regulator 18, regulator 18 may transmit an event indicator 82 to security server 50. Server 50 may further formulate and communicate an event notification 83 to administrator device 20 for display to the administrator. In some embodiments, notification 83 is communicated to device 20 using a push protocol. In response to the event, security server 50 and/or administration device 20 may operate changes to the configuration parameters used by client system 12 and/or network regulator 18 to protect client system 12. In one such example, when server 50 determines that client system 12 comprises malware, it may instruct network regulator 18 to restrict access of the respective client system to networks 14 and/or 16. Such configuration changes may be communicated as updated configuration settings 80. Fig. 12 shows an exemplary sequence of steps performed by security server 50 and/or administration device 20 to carry out an event notification.

[0069] Figs. 13-A-B show an exemplary sequence of steps performed by administration application 64 according to some embodiments of the present invention. Application 64 exposes GUI 65, which enables the administrator to remotely manage client system 12 and/or to configure protection of client system 12. In a device management view, some embodiments of GUI 65 enable the administrator to associate a device name, a visual ID, and an owner with each protected client system. Exemplary visual IDs include, among others, a photograph of the owner, an icon (e.g., symbol, avatar) of the owner, a photograph of the respective client system, or an arbitrary image used as a mnemonic for the owner and/or the respective client system. The GUI may subsequently represent the respective client system using the respective name, visual ID, etc.

[0070] Such associations between the protected client system and a visual ID/icon may facilitate device administration, especially when the administrator is not particularly skilled in system or network administration or computer security. In particular, some embodiments allow the administrator to associate each protected client system with an address book entry. When administration device 20 is a smartphone, such associations provide a quick and convenient mechanism of contacting the owner of a protected system, for instance to communicate the occurrence of a security event, or to enquire about a security event involving the respective client system.

[0071] Fig. 14 shows an exemplary sequence of steps performed by administration application 64 to display an event notification within GUI 65, according to some embodiments of the present invention. Displaying the notification may comprise displaying a device name and a name of the owner of the respective client system, and displaying a visual ID (icon) associated with the owner. Also, in some embodiments, the name and/or icon of the owner may be hyperlinked to a communication interface of device 20 (e.g., a telephone call interface, e-mail interface, messaging interface, etc.). When the administrator activates (e.g., clicks, touches) the respective hyperlink, the respective communication interface may be invoked, instantiated with the contact details of the owner of the client system indicated by the current notification.

[0072] Fig. 15 shows a snapshot of a device management view generated by GUI 65 according to some embodiments of the present invention. Fig. 15 shows an exemplary display of

information related to network regulator **18**. GUI **65** may display a top-level menu including buttons **84a-c** that invoke a notification GUI, a device status/configuration GUI, and a service/subscription information GUI, respectively.

[0073] Fig. **16** shows another exemplary snapshot of the device management view, the snapshot illustrating an initial configuration (setup) of a protected client system – in this case, a thermostat. The exemplary device management view displays a device icon **85** indicative of the respective client system, an owner icon **86** associated with the owner, and a device name **87** of the respective client system. Figs. **17-A-B** show device configuration screens accessed via the interface illustrated in Fig. **16**. The interface illustrated in Fig. **17-A** enables the administrator to assign the current client system to a pre-determined device group **90** (e.g., family/ guest). In some embodiments, members of each device group **90** have group-specific values of configuration parameters. For instance, in some embodiments, for members of the “guest” group, GUI **65** does not allow configuration of device management parameters. In the example of Fig. **17-A**, for members of the “family” group, GUI **65** offers the administration a choice of whether to activate device management for the current client system or not. Fig. **17-B** shows an interface enabling the administrator to select a network connection speed for the current client system, from a set of available options.

[0074] Fig. **18** shows an exemplary snapshot of the device management view, illustrating a manner in which GUI **65** may enable the administrator to associate the current client system with an owner and/or with a visual ID/icon. In some embodiments, GUI **65** allows the administrator to select the owner from a contacts list (e.g. Address Book).

[0075] Fig. **19** shows an exemplary snapshot of the device management view, illustrating a manner of displaying information about a protected client system. The available information may be grouped into sections, such as “Device”, “Safety”, and “Performance”, among others. GUI **65** may visually represent the respective client system using device-specific icon **85** (here indicating a personal computer), device name **87**, owner name **88**, and visual ID **86** associated with the owner. The exemplary view of Fig. **19** may further show a location indicator **89** indicating whether the respective client system is currently connected to its home network (e.g. local network **14** protected by network regulator **18**), or is out of the range of network **14**. When

the respective client system is not currently connected to its home network, some embodiments of location indicator **89** may further show whether the respective client system is currently protected using VPN.

[0076] Figs. **20-A-B** show exemplary snapshots of the device management view generated by GUI **65**, illustrating further information and/or configuration parameters and current values set for the current client system. In some embodiments, the device management view may display a group of vulnerability assessment indicators **91** determined for the current client system. Vulnerability data may be determined by a management agent executing on client system **12** and transmitted to client configuration server **52** (see, e.g., item **81** in Fig. **9**). Vulnerability assessment indicators **91** may include a password quality indicator **92** and a list of system vulnerabilities, further illustrated in Fig. **20-B**.

[0077] Fig. **21** shows an exemplary snapshot of the device management view of GUI **65**, the view displaying a list of protected client systems. Each such client system may be represented using a device icon, device name, owner's name, and owner icon associated with the owner of the respective client system.

[0078] Figs. **22-A-B** show exemplary snapshots of a notification view generated by GUI **65** according to some embodiments of the present invention. The illustrated notification view displays a list of event notifications. In some embodiments, event notifications are represented using a device icon, device name, owner's name, and owner icon associated to the respective client.

[0079] In some embodiments, more details about each event notification may be accessed by clicking (or touching) a GUI element such as an icon or the screen area containing the respective notification. A snapshot of a notification view displaying such details is shown in Fig. **23**. Details displayed in relation to the selected notification may include an indicator of a type or category of event (e.g., "Website blocked"), and a time stamp. In some embodiments, a text definition **93** is provided to describe the respective type/category of event. Text definition **93** may be formulated to give the administrator an understanding of the respective event and of its urgency, importance, and potential consequences. Including such information in the notification may allow a person who is not particularly skilled in network management and computer

security to use administration application **64** to remotely manage client systems **12a-f** and/or network regulator **18**.

[0080] Figs. **24-A-B** show an exemplary notification view displayed in relation to device maintenance events (e.g., a software update notification and a disk cleanup notification, respectively). Some embodiments of the present invention display such maintenance notifications alongside security notifications (see, e.g. Fig. **22-A-B**), allowing the administrator to manage security and device functionality from a single, unified interface.

[0081] In some embodiments, a device management view and a notification view generated by GUI **65** employ distinct manners of visually communicating information. For instance, each view may choose to emphasize a different visual element, such as an icon. Emphasizing a visual element herein means deliberately rendering the respective element in a manner that makes the respective element stand out in comparison with other visual elements on screen. Emphasizing a visual element may be achieved in many ways. For instance, to emphasize an icon, the icon may be scaled up to occupy a bigger area of the display than other visual elements. Emphasized elements may be rendered in brighter or more saturated colors than other elements. To emphasize a piece of text (e.g., a name), the respective text may be rendered in boldface or in a bigger font size, etc.

[0082] In some embodiments of a device management view, the device icon may be emphasized with respect to the owner icon. In contrast, in a notification view, the owner icon may be emphasized with respect to the device icon. An example of such selective, view-specific emphasizing is seen in Figs. **19** and **23**. Such a manner of presenting information may be more empathic and human-centric than others, and may appeal more to non-technical users.

[0083] The exemplary systems and methods described herein allow protecting a plurality of client systems against computer security threats, such as malicious software and network intrusion. Besides protecting conventional computer systems, the described systems and methods are particularly suited for protecting a diverse ecosystem of intelligent devices connected to the Internet, such as devices collectively known in popular culture as the Internet of Things (IoT). Examples of such devices include, among others, wearable devices (e.g., smartwatches, fitness bands, interactive jewelry), home entertainment devices (TVs, media

players, game consoles), home appliances (refrigerators, thermostats, intelligent lighting systems, home security systems). Some embodiments allow, for instance, protecting all electronic devices in a home using a unified, integrated solution.

5 [0084] Some embodiments include a network regulator configured to set up and manage a local network interconnecting the plurality of protected client systems. The network regulator may install itself in a position of gateway between the local network and an extended network such as the Internet. In some embodiments, protection is achieved by the network regulator re-routing at least a part of data traffic exchanged between a protected client system and an entity outside the local network through a remote security server. The traffic may then be scanned for malware,
10 and access to risky resources (e.g., malicious or fraudulent websites) blocked.

[0085] In some embodiments, the network regulator is uniquely associated with a service subscription, which allows a unified management of security and other aspects for all protected client systems, e.g., for all intelligent devices within a home. A security event, such as an attempt by a protected client system to access a fraudulent website, may thus be automatically
15 associated with a subscription account, and reported to a contact person/administrator of the respective account. Reporting of security events may comprise sending a notification to an administration device (e.g., mobile phone) of the administrator. In some embodiments, such notifications are centralized by the security server and grouped per user and/or per device. A graphical user interface (GUI) executing on the administration device may display information
20 about each security event, statistical data, etc. Some embodiments of the present invention therefore allow a centralized solution for managing computer security for a large number of customers/accounts, each such account associated with its own diverse group of devices.

[0086] Aside from ensuring protection of client systems connected to the local network, some embodiments provide a unified solution for automatic configuration, troubleshooting/technical
25 assistance, and remote management of the protected client systems. Some embodiments install a utility agent on each protected device, the utility agent collaborating with remote servers to receive configuration data and/or executable code. The user/administrator of a client system may remotely manage the respective device via a user interface displayed on an administration device (e.g., mobile phone). Such management may include, for instance, setting operational

parameters (a desired home temperature, a parental control setting, etc.), applying software updates, and troubleshooting.

[0087] Some embodiments of the present invention are specifically crafted for ease of use, so as to not necessitate specialized knowledge of computer engineering or network administration.

5 For instance, upon installation, the network regulator may automatically take over some network services from an existing router, to become the default provider of Internet access for the local network.

[0088] It will be clear to a skilled artisan that the above embodiments may be altered in many ways without departing from the scope of the invention. Accordingly, the scope of the invention

10 should be determined by the following claims and their legal equivalents.

CLAIMS

What is claimed is:

1. A computing system comprising a hardware processor and a memory, the memory storing instructions which, when executed by the hardware processor, cause the computing system to:
 - receive data from a remote server, the data selected by the server for transmission to the computing system according to a subscription associated with a network regulator protecting a plurality of client systems against computer security threats, wherein the plurality of client systems are connected to the network regulator over a local network; and
 - perform a display of a graphical user interface (GUI) configured to:
 - generate a device management view enabling a user to remotely configure a client system of the plurality of client systems, and
 - generate a security notification view displaying an indicator of a security event caused by an action of the client system,
 - wherein the network regulator is configured, in response to connecting to a router providing a network service to the plurality of client systems, to automatically take over the network service from the router, wherein the network service comprises supplying network addresses to the plurality of client systems.
2. The computing system of claim 1, wherein both the device management view and the security notification view display an owner icon and a device icon, the owner icon symbolizing an owner of the client system and the device icon symbolizing the client system, and wherein:
 - generating the device management view comprises displaying the owner icon and the device icon in a manner which emphasizes the device icon with respect to the owner icon; and

generating the security notification view comprises displaying the owner icon and the device icon in a manner which emphasizes the owner icon with respect to the device icon.

3. The computing system of claim 1, wherein the device management view displays an interactive element enabling a user to select a contact from a list of contacts used by the computer system, and to designate the contact as owner of the client system.

4. The computing system of claim 1, wherein the device management view displays a vulnerability indicator indicative of how susceptible the client system is to computer security threats, the vulnerability indicator selected from a group consisting of an indicator of a quality of a password protecting the client system, and an indicator of whether a software executing on the client system is up to date.

5. The computing system of claim 1, wherein the device management view displays an interactive element which, when activated by a user of the computing system, causes a transmission of a notification to the client system, the notification causing the client system to update a software component executing on the client system.

6. The computing system of claim 1, wherein the device management view displays an interactive element which, when activated by a user of the computing system, causes a transmission of a notification to the network regulator, the notification causing the network regulator to update a software component executing on the network regulator.

7. The computing system of claim 1, wherein the security event comprises detecting malicious software executing on the client system.

8. The computing system of claim 1, wherein the security event comprises detecting an attempt by the client system to access a resource located outside the local network,

3 wherein accessing the resource constitutes a computer security threat to the client
4 system.

5
1 9. The computing system of claim 1, wherein the indicator of the security event comprises
2 an indicator of a category of computer security threats indicated by the security event,
3 and further comprises a text definition of the category.

4
1 10. The computing system of claim 1, wherein the computing system comprises a mobile
2 telephone.

3
1 11. A method comprising:

2 employing a network regulator to protect a plurality of client systems against computer
3 security threats, wherein the plurality of client systems are connected to the
4 network regulator over a local network;

5 employing the network regulator, in response to connecting to a router providing a
6 network service to the plurality of client systems, to automatically take over the
7 network service from the router, wherein the network service comprises supplying
8 network addresses to the plurality of client systems;

9 in response to the network regulator taking over the network service, employing a
10 hardware processor of a computing system to receive data from a remote server,
11 the data selected by the server for transmission to the computing system according
12 to a subscription associated with the network regulator; and

13 in response to the network regulator taking over the network service, employing the
14 hardware processor to perform a display of a graphical user interface (GUI)
15 configured to:

16 generate a device management view enabling a user to remotely configure a client
17 system of the plurality of client systems, and

18 generate a security notification view displaying an indicator of a security event
19 caused by an action of the client system.
20

12. The method of claim 11, wherein both the device management view and the security notification view display an owner icon and a device icon, the owner icon symbolizing an owner of the client system and the device icon symbolizing the client system, and wherein:

generating the device management view comprises displaying the owner icon and the device icon in a manner which emphasizes the device icon with respect to the owner icon; and

generating the security notification view comprises displaying the owner icon and the device icon in a manner which emphasizes the owner icon with respect to the device icon.

13. The method of claim 11, wherein the device management view displays an interactive element enabling a user to select a contact from a list of contacts used by the computer system, and to designate the contact as owner of the client system.

14. The method of claim 11, wherein the device management view displays a vulnerability indicator indicative of how susceptible the client system is to computer security threats, the vulnerability indicator selected from a group consisting of an indicator of a quality of a password protecting the client system, and an indicator of whether a software executing on the client system is up to date.

15. The method of claim 11, wherein the device management view displays an interactive element which, when activated by a user of the computing system, causes a transmission of a notification to the client system, the notification causing the client system to update a software component executing on the client system.

16. The method of claim 11, wherein the device management view displays an interactive element which, when activated by a user of the computing system, causes a transmission of a notification to the network regulator, the notification causing the network regulator to update a software component executing on the network regulator.

- 6
- 1 17. The method of claim 11, wherein the security event comprises detecting malicious
2 software executing on the client system.
- 3
- 1 18. The method of claim 11, wherein the security event comprises detecting an attempt by
2 the client system to access a resource located outside the local network, wherein
3 accessing the resource constitutes a computer security threat to the client system.
- 4
- 1 19. The method of claim 11, wherein the indicator of the security event comprises an
2 indicator of a category of computer security threats indicated by the security event,
3 and further comprises a text definition of the category.
- 4
- 1 20. The method of claim 11, wherein the computing system comprises a mobile telephone.
- 2
- 1 21. A non-transitory computer-readable medium storing instructions which, when executed
2 by a hardware processor of a computing system, cause the computing system to:
3 receive data from a remote server, the data selected by the server for transmission to the
4 computing system according to a subscription associated with a network regulator
5 protecting a plurality of client systems against computer security threats, wherein
6 the plurality of client systems are connected to the network regulator over a local
7 network; and
8 perform a display of a graphical user interface (GUI) configured to:
9 generate a device management view enabling a user to remotely configure a client
10 system of the plurality of client systems, and
11 generate a security notification view displaying an indicator of a security event
12 caused by an action of the client system,
13 wherein the network regulator is configured, in response to connecting to a router
14 providing a network service to the plurality of client systems, to automatically
15 take over the network service from the router, wherein the network service
16 comprises supplying network addresses to the plurality of client systems.
- 17