SYSTEM AND METHOD FOR NETWORK-LEVEL SMART HOME SECURITY

FIG. 5
SYSTEM AND METHOD FOR NETWORK-LEVEL SMART HOME SECURITY

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application is a non-provisional of, and claims benefit under 35 U.S.C. §119(e) from, U.S. Provisional Application No 62/310,405, filed March 18, 2016 and entitled “System and Method for Network-Level Smart Home Security”.

BACKGROUND

[0002] With new smart home platforms such as HomeKit (from Apple) and Brillo/Weave (from Google), smart home technology is rapidly entering the mainstream of consumer consciousness. Connected devices, which may be available from a myriad of vendors, include HVAC controls, lighting, home entertainment devices, health and wellness devices, home security, and more. Typically, to function in the context of a smart home, these devices are configured for network connectivity.

[0003] Further, many of these devices may utilize connectivity from outside the home network in order to reach their full potential. For example, a user may control lighting while away in order to deter burglars or may activate air conditioning before arriving at home. In order to achieve this remote access, many smart home devices are exposed to the public Internet to realize their full functionality, meaning that traffic initiated from the exterior of the home network may need to be allowed to pass the home’s router/NAT gateway and be routed to the device on the interior of the home network.

[0004] In many smart home devices, this process is facilitated via mechanisms such as NAT-PMP or UPnP Port Mapping, or via a Web-based forwarding service, which allow connected devices to tell the router how traffic from the external network may be routed into the network interior. Once on the network, however, these devices are exposed to the public internet, meaning that they are vulnerable to port-scans, password guessing, malware attacks and other security risks. Further, while many such devices may have passwords set, these are often weak passwords, unchanged by users, and re-used by vendors.

[0005] Many home networks have a default firewall in place which is implemented at their router. It is the task of the firewall to block access to devices on the interior of the network. However, configuring the necessary access controls for a firewall to establish the pinholes that will allow selected traffic is both difficult from a user experience perspective, and requires that users know ahead of time the IP address ranges of remote networks that may need to access smart home devices in the interior of the network.
The current approach of exposing smart home devices to the entire public Internet is an extremely coarse-grained and risky technique for allowing remote access. The risks associated with such an approach may be compounded by the fact that an increasing number of smart home devices present physical security and privacy threats if they are compromised. For example, although a home baby camera may be a device that householders validly wish to monitor from outside the home network; if compromised, this device threatens the privacy of those in the home, as it allows attackers to watch the family in their home.

Likewise, while remote access to devices such as smart door locks or home alarm systems provides great utility (as householders can let themselves in if they’ve forgotten a key, or unlock a door if a cleaning service or visitor requires access), this same remote access can present a serious security threat if attackers gain control over it. By probing a door lock for security weaknesses remotely, attackers can launch automated attacks that can give them access to the physical site of the home, often without householders even being aware of the fact that their security has been compromised.


To mitigate such risks, device vendors provide some basic security policies that are intended to ensure that only householders can access these devices remotely. For example, device vendors may use a password mechanism, such that while the device can be contacted from anywhere on the Internet, only those with the correct password may log in to access it. This approach is problematic, however, as research has demonstrated that users often choose extremely weak passwords, or—even worse—do not change passwords from the default settings. Most common Linksys routers, for example, use a default username/password combination of “admin/admin”. Many other devices use similarly weak passwords, which are often well known to hackers. Some other devices may use Secure Shell (SSH) for more secure access, but such use is often with the same private key on all devices. These poor security practices make it so that hackers can even locate Internet-connected devices with unchanged default passwords through a
simple Google search, books have been written on how to do this (see, for example, Johnny Long et al., Google Hacking for Penetration Testers (3d ed. 2015)).

[0010] Beyond poor password security, these devices are also at risk from software vulnerabilities that may allow them to be remotely compromised if an attacker can reach them over the network. Heartbleed, Gatekeeper, and other recently discovered vulnerabilities have shown that even desktop-grade computer software can have lurking bugs that are difficult to find. The threat may be much greater for smart home devices, given the diversity of vendors involved, the varying levels of secure software development practices, and—all too often—the lack of available or easy-to-apply software patches once vulnerabilities are discovered. Dan Goodin, *9 baby monitors wide open to hacks that expose users’ most private moments*, Ars Technica (Sept. 2, 2015), https://arstechnica.com/security/2015/09/9-baby-monitors-wide-open-to-hacks-that-expose-users-most-private-moments/.

[0011] While Firewalls and other software technologies protect desktop and laptop computers from certain types of remote access, these technologies are generally not present on low-cost embedded smart home devices. Also, note that typical home network security recommendations, such as enabling WPA encryption on the wireless network, do not protect against these risks. This is because, even though the home wireless network may be protected, smart home devices are typically designed so that they are accessible from outside that secure network.

[0012] Finally, in at least some scenarios, Firewalls present two additional challenges. The first is based in user experience problems: configuring access control rules for a home router may be far beyond the ability of non-technically inclined consumers (and even many technically inclined consumers). It generally requires determining the router’s IP address, connecting to it from a browser, authenticating, navigating to the correct tabs, and understanding arcana around remote IP addresses, network ranges, port forwarding, DMZ restrictions, and so forth. The second challenge is that, even if a user does understand how to properly configure his or her firewall, in some scenarios, the remote IP address information must be known ahead of time in order to perform the configuration. In other words, if a user will be staying at a hotel on a business trip, there is generally no way to set up the firewall correctly before leaving on the trip, since the user will not know the IP addresses in use by the hotel’s remote network.

[0013] What is needed is a way to provide remote network access to smart home devices, but with tighter controls over which remote networks can access those devices. These controls should be implemented in a way that is easy to use for non-technical users and does not require explicit additional configuration (prior research shows that, even though consumers care about security
and privacy, they are often unwilling to take explicit steps to protect themselves if such steps trade off against usability or convenience).

**OVERVIEW**

[0014] Systems and methods disclosed herein describe an approach to increase the security of smart homes, specifically the connected devices and services that are becoming increasingly prevalent. The mechanism described herein restricts network access to devices and services in the interior of the home network by securely provisioning which remote IP addresses are allowed access. Since this approach uses network-level (rather than application-level) mechanisms, it can protect even smart home devices that may have weak built-in security controls.

[0015] Smart home devices typically are accessible remotely, and yet the only mechanisms conventionally available to allow such remote access are too coarse-grained, or too hard to use, and/or exposes these devices to the entire public Internet. This may make them targets for port-scanning, malware injection, and repeated password cracking attempts, among other concerns.

[0016] One way to mitigate these risks would be to restrict network-level access so that only certain remote IP addresses are allowed to access devices on the interior of the network. These configurations are sometimes called firewall pinholes because they allow traffic from a certain remote IP address to access only certain devices in the network interior. This would prevent random attackers from anywhere on the Internet attempting to circumvent security. But the allowed remote IP addresses still need to be specified. The common way in firewalls today is for users to explicitly whitelist all allowable IP addresses that are allowed to connect to home network devices. Such an approach would not only be tedious and error prone (and likely not feasible for non-technically inclined users), but may also not work in some situations in which users did not know ahead of time where they would be accessing the system from.

[0017] So, in order to limit remote access to smart home devices in a way that is actually feasible and workable, it is desirable to use implicit mechanisms through which users can easily establish, at the time of need, that a given IP address should be allowed access to some device or devices on the home network. This mechanism would then enable the home network to accept a connection request from the newly approved remote IP address, and allow connections from it to the device in the interior of the home network. If any other IP addresses, from any other locales, attempt to connect, the connection request would be silently dropped, making home devices invulnerable to remote attacks from other networks.

[0018] Because the access control functions at the network level, at least some of the various embodiments described herein can be implemented for numerous smart home devices and may not
rely on support or cooperation from the vendors of those devices. At least some of the various embodiments described herein are particularly advantageous because they can protect devices that may have extremely poor application-level security features (such as default passwords, or software vulnerabilities) by restricting access to these devices at the network level.

[0019] At least one embodiment works as follows. One device, designated as the access device, is used to remotely configure network-level access to the home network, at a time such access is needed. The access device may be, for example, a mobile phone or laptop or other arbitrary computing device. The access device cooperates with software on the home router in order to securely provision access as needed.

[0020] The first step in this process, the set-up phase, may occur only once, and is the creation of a secure association between the access device and the home router. During this step (in this exemplary embodiment) signed digital certificates are exchanged between these two devices; this exchange allows either of them to securely and cryptographically verify the identity of the other in the future. The certificates are also used to encrypt or to facilitate encrypting network communication between the two devices.

[0021] This exchange (e.g., one-time exchange) of certificates can happen using any variety of mechanisms, such as, for example, near-field communication (NFC) (the access device is brought into contact with the router), Bluetooth, USB key, and/or infrared or audio-based communications, among other approaches.

[0022] Once this exchange occurs, the access device can communicate securely with the home router, and authenticate its identity to the router as needed, even when the device is outside the home, on a remote network.

[0023] Following this, the home router creates a device inventory of the devices and/or services in the interior of the home network, which may ultimately serve as destinations for inbound Internet traffic. This inventory is periodically transmitted to the access device so that it has an up-to-date database of smart home devices to which it can provide access.

[0024] Following the set-up phase, the user can specify that remote access should be allowed from a given network by bringing the access device into that network and running an application (sometimes referred to herein as a remote access app or app) installed on the device. This application establishes a secure connection back to the user’s home network and connects to the home router there. The access device assesses its current IP address and the network configuration of the remote network, and transmits this information securely back to the home router. The home
router then uses this information to add an access control rule that allows traffic from the remote network to transit the router and connect to the smart home device on the interior of the network.

[0025] In at least this example embodiment, simply running the application on the access device collects and securely provides to the router the remote-access information the router uses for configuring its network-layer security access control rules. At this point, devices on the remote network are allowed to access the smart home device. Other devices, with IP addresses outside of this remote network, are not allowed to connect.

[0026] Optionally, at the time the application is run, the user can specify whether the remote network should be allowed to always access the smart home device (which may be the case if remote family members, such as grandparents, are to be given access to a baby monitor camera), or only temporarily access it (such as might be the case if the user is accessing the baby camera from a hotel Internet connection). The user can also optionally specify that the remote network can access all smart home devices, or only a restricted set of devices, and/or configure other policies as described later.

[0027] Once set up, the home router silently drops any connection requests from unauthorized remote networks. However, devices on authorized networks are allowed to connect, and the router rewrites the headers of both inbound and outbound traffic to ensure that source and destination addresses and port are set up properly. New authorization rules can be added at any time by simply taking the access device to a new network and adding that network as an allowable source.

[0028] Building on these basic steps, there are many variants possible which are detailed later in this disclosure.

[0029] In many scenarios, there are both security and user interface advantages to the various embodiments described herein.

[0030] From the security perspective, at least some of the embodiments described herein are advantageous because they enhance the security of remote access for all smart home devices on the home network, including even for devices that may be rife with other security problems. In other words, at least some embodiments provide an additional layer of security without requiring that vendors patch their code or without requiring that users set strong passwords. By addressing the problem at the network layer, rather than the application layer, at least some embodiments described herein simply disallow access from remote networks that aren’t approved by the user.

[0031] At least some embodiments described herein also have the advantage that they defend against malware on smart home devices more effectively than alternative approaches. Even a smart home device with robust authentication checks (such as strong passwords) typically needs to still
be connectable over the Internet, meaning that—even if an attacker never tries to authenticate to the device—the device may still be vulnerable to security-related software bugs that can be a vector for malware. By preventing even the attempt at connection, at least some embodiments described herein effectively place these vulnerable devices behind a firewall, albeit one that is configured without dealing with tedious and technically complex network configuration screens.

[0032] From a user interface perspective, at least some embodiments described herein are advantageous over competing approaches because of their simplicity. In such embodiments, there are no complex network security rules to administer in the home router configuration, yet the level of protection provided by the present disclosure is comparable to a well-configured firewall. Further, access can be granted (e.g., by the system) to devices from remote networks at the time the access is needed, rather than requiring that users remember to pre-configure their network configuration rules. This means the present disclosure works for remote networks whose IP addresses are not known ahead of time.

[0033] Additional embodiments described herein allow for users to dictate whether permanent or transient/ephemeral access from certain remote networks should be granted, and to determine which set of devices should be accessible from which remote network. Notifications can also be used to allow users to determine in real-time whether a given access should be granted.

[0034] One known method of externally opening ports on a firewall is known as port knocking, which involves generating a sequence of connection attempts from outside the firewall to a pre-specified sequence of closed ports. Once a correct sequence of connection attempts is received, the firewall rules are dynamically modified to allow the host that sent the connection attempts to connect over specific port(s). This is different from aspects of the present systems and methods, which, in at least one embodiment, involve adding external IP addresses to a whitelist on a firewall (e.g., gateway) by presenting a certificate/secret obtained via the LAN side of the firewall upon connection to a specified service port not affected by the whitelist. Once a proper certificate/secret has been presented, the firewall whitelist is dynamically modified to allow traffic to all open ports from the source IP address of the connection.

[0035] Among the advantages of at least some embodiments of the present disclosure is that only the access (control) device and the home gateway have to have additional intelligence. That is, in at least one or more embodiments, the present systems and methods use the access device (e.g., a mobile device) that has moved to a remote network to enable (using the shared secrets/certificates) one or more other devices on that remote network to connect to one or more devices that are on the LAN behind the firewall/gateway without those one or more other devices
on that remote network having to change their configuration in any way. The approach of the present methods and systems is also less complex than SSH port forwarding.

[0036] In at least one embodiment, a router according to the present systems and methods is configured by default to block outside traffic unless it comes from a whitelisted address. In at least one other embodiment, a router according to the present systems and methods is configured by default to allow all traffic until the local-certificate-exchange procedure has occurred, and thereafter blocking outside traffic unless it comes from a whitelisted address. And certainly other possibilities could be listed here as well.

**BRIEF DESCRIPTION OF THE DRAWINGS**

[0037] FIG. 1A is a flow diagram illustrating an overview of data flow and/or data processing of an example set-up phase, in accordance with at least one embodiment.

[0038] FIG. 1B is a flow diagram illustrating an overview of data flow and/or data processing of an example implicit-authorization phase, in accordance with at least one embodiment.

[0039] FIG. 1C is a flow diagram illustrating an overview of data flow and/or data processing by an example router of inbound and outbound traffic, in accordance with at least one embodiment.

[0040] FIG. 2 is a flowchart depicting an exemplary embodiment of this process of determining remote network configuration parameters.

[0041] FIG. 3 is an illustration of an example user interface for allowing users to indicate access policies, in accordance with at least one embodiment.

[0042] FIG. 4A is a flow diagram illustrating the flow and/or processing of example inbound traffic by an example router, in accordance with at least one embodiment.

[0043] FIG. 4B is a flow diagram illustrating the flow and/or processing of outbound traffic by an example router, in accordance with at least one embodiment.

[0044] FIG. 5 is a flow diagram illustrating access control to a local area network (LAN) from a wide area network (WAN), in accordance with at least one embodiment.

[0045] FIG. 6 is a flow chart depicting an example method of controlling access to a local area network (LAN) from a wide area network (WAN), in accordance with at least one embodiment.

[0046] FIG. 7 illustrates an exemplary wireless transmit/receive unit (WTRU) that may be employed as an access device, in accordance with at least one embodiment.

[0047] FIG. 8 illustrates an exemplary network entity that may be employed as a home router, in accordance with at least one embodiment.
DetaIled Description

[0048] An exemplary embodiment disclosed herein provide a mobile phone being used as the access device.

[0049] In at least one embodiment, a set-up phase is included. FIG. 1A is a flow diagram illustrating an overview of data flow and/or data processing of an example set-up phase, in accordance with at least one embodiment.

[0050] The depicted embodiment includes a home network 102, an access device 104, and a home router 106. In at least one embodiment, the set-up phase is executed at least once for the access device 104. In at least one embodiment, the set-up phase is executed when the access device 104 is present in the user's home network 102.

[0051] In at least one embodiment, the set-up phase establishes a cryptographically secure identity and communications between the access device 104 and home router 106. In at least one embodiment, the home router 106 collects device inventory information of devices and services on the home network and periodically updates the access device 104 with this database.

[0052] During the set-up phase, in at least one embodiment, the access device 104 and the home router 106 each generate cryptographic keys (at 120, 122), using a common public-key encryption algorithm. For example, the access device 104 may generate a public/private key pair and/or the home router 106 may generate a public/private key pair.

[0053] In at least one embodiment, the public keys are then bundled into a digital certificate for each device, which is then signed by each device (at 124, 126).

[0054] In at least one embodiment, these digital certificates are then exchanged between the two devices, such that the access device 104 holds a copy of the home router 106’s certificate, and the home router 106 holds a copy of the access device 104’s certificate (at 128, 130). Both devices store the private keys generated.

[0055] The communication process by which these certificates are exchanged can vary. In an exemplary embodiment, an approach that provides for a degree of physical security—such as using near-field communication (NFC) and/or other location-limited communication technologies—is employed. Of course, other approaches may be employed, such as, for example, exchanging the certificates using a USB key, emailing them to the respective devices, and/or “manually” filling them in via a form interface.

[0056] After the set-up phase, in at least one embodiment, both the access device 104 and the home router 106 can verify the identity of the other, even when the home router 106 and the access
device 104 are remote from each other. In at least one embodiment, the public/private key information contained in the certificates, and stored on the devices, can be used to securely encrypt future network communications between the two.

[0057] In at least one embodiment, a device-inventory phase is included. In at least one embodiment, the home router 106 creates a device inventory (at 132). In at least one embodiment, the device inventory details some or all of the devices and/or services in the interior of the home network 102 that may ultimately serve as destinations for inbound Internet traffic. Collecting the device inventory information allows, for example, users to create the desired security configurations on the router 106, as described shortly.

[0058] In at least one embodiment, the device inventory information is periodically transmitted to the access device 104 (at 134). The device inventory information is transmitted to the access device 104, for example, so the access device 104 can create a user interface with an up-to-date list of some or all possible smart home devices to which access can be configured (e.g., by the access device 104). And certainly other possibilities may be implemented as well.

[0059] In at least one embodiment, the router 106 is configured to collect the MAC addresses of every client device on the home network. In at least one embodiment, the router 106 is configured to obtain this information, via the tables of link-layer (MAC) addresses that are used to implement Reverse Address Resolution Protocol (RARP), Bootstrap Protocol (BOOTP), or Dynamic Host Configuration Protocol (DHCP), which are common protocols in existing home networks that provide mappings from link-layer to network-layer addresses (for example, from MAC addresses to IP addresses). In at least one embodiment, these databases are automatically maintained by the router, as new client devices connect to and disconnect from the home network 102. In at least one embodiment, the tables are manually updated on the router.

[0060] In at least one embodiment, the database-inventory phase results in a table that maps link-layer addresses to network-layer addresses. Immediately below is an exemplary embodiment of such a table:

<table>
<thead>
<tr>
<th>LINK-LAYER ADDRESS</th>
<th>NETWORK-LAYER ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:13:10:0F:BC:29</td>
<td>192.168.1.24</td>
</tr>
<tr>
<td>00:25:9C:84:22:A9</td>
<td>192.168.1.10</td>
</tr>
<tr>
<td>68:74:74:F1:12:C9</td>
<td>192.168.1.54</td>
</tr>
</tbody>
</table>

[0061] In at least one embodiment, a scanning-process phase is included. Following the database-inventory phase, in at least one embodiment, the router 106 is configured to scan the
client devices on the home network 102 to determine the device name as well as any open ports on the device, which indicate services available for connection. In at least one embodiment, the router 106 is configured to include one or more network scanning tools, such as for example, Nmap. The router 106 may be configured to carry out the scanning-process phase, at least in part, by running one or more features of the networking scanning tool, such as, for example, target specification, host discovery, and/or port scanning, among others. In an exemplary embodiment, this information is represented in a table that is indexed by network-layer address and contains a relation mapping that network-layer address to the name of the device and any open service ports. In at least one embodiment, devices with multiple open service ports are represented using multiple rows in the table. For example:

<table>
<thead>
<tr>
<th>NETWORK-LAYER ADDRESS</th>
<th>DEVICE NAME</th>
<th>SERVICE PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.24</td>
<td>Nest Thermostat: Living Room</td>
<td>2304</td>
</tr>
<tr>
<td>192.168.1.10</td>
<td>Linksys Babycam</td>
<td>80</td>
</tr>
<tr>
<td>192.168.1.10</td>
<td>Linksys Babycam</td>
<td>1991</td>
</tr>
</tbody>
</table>

[0062] In at least one embodiment, the information obtained from the device-inventory phase and the scanning-process phase is combined via a relational join operation, creating a unified device inventory database on the router that maps from unique link-layer addresses to device name and port information. For example:

<table>
<thead>
<tr>
<th>LINK-LAYER ADDRESS (UNIQUE DEVICE IDENTIFIER)</th>
<th>DEVICE NAME</th>
<th>SERVICE PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:13:10:0F:BC:29</td>
<td>Nest Thermostat: Living Room</td>
<td>2304</td>
</tr>
<tr>
<td>00:25:9C:84:22:A9</td>
<td>Linksys Babycam</td>
<td>80</td>
</tr>
</tbody>
</table>

[0063] In at least one embodiment, the link-layer address for each device is unchanging and thus can serve as a unique device identifier for each device.

[0064] The updated database may be stored on one or more of several mediums. In at least one embodiment, the updated database is stored in the router 106’s memory or flash storage. In at least one embodiment, the updated database is periodically transmitted to the access device 104. In at least one embodiment, the security credentials configured into both the access device 104 and the
home router 106 allow these database updates to be transmitted securely and confidentially at any point in the future.

[0065] In at least one embodiment, the router 106 then creates at least two additional databases (at 136, 138). The additional databases may be initially empty. In at least one embodiment, the first database is a translation table (T/T) database. The translation-table database may be used to maintain information about how to translate IP header information as packets cross between the interior and exterior of the network. In at least one embodiment, the second database is an access rules (A/R) database. The access-rules database may contain security rules about which external IP addresses are allowed to connect.

[0066] In at least one embodiment, an implicit-authorization phase is included. In at least one embodiment, the translation-table database and the access-rules database are updated during the implicit-authorization phase and are used to correctly maintain traffic flows between the home network and the Internet during network accesses, while ensuring security.

[0067] In at least one embodiment, after the creation of the translation-table database and the access-rules database, the router 106 enters a “steady state” mode where access from any remote IP address is automatically blocked by the router 106, preventing unintended access to any of the devices and services on the home network 102.

[0068] As disclosed above, the implicit-authorization phase is the process of collecting the information for configuring the home router 106 to securely permit access to the home network 102, and securely transmitting this information back to the home router 106. FIG. 1B is a flow diagram illustrating an overview of data flow and/or data processing of an example implicit-authorization phase, in accordance with at least one embodiment. FIG. 1B depicts how the access device may provision access from devices on a remote network to devices on the interior of the home network, securely. In at least one embodiment, the access device determines the configuration of the remote network, the approved destination devices back in the user’s home network, as well as user policy desires, and transmits these to the home router. The router then updates its translation table database and access rule database, allowing devices on the same remote network as the access device to establish connections into the interior of the home network.

[0069] In at least one embodiment, during the implicit-authorization phase, the information is collected by the access device 104 during or after the set-up phase. The information may be collected multiple times, for example, if a user wishes to provide remote access from multiple networks to devices on the home network 102.
[0070] There are a number of embodiments within the implicit-authorization process. In at least one embodiment, the access device 104 determines an “approved” remote IP address—or range of remote IP addresses—that will be allowed to connect to one or more devices in the interior of the home network 102. In at least one embodiment, this information is collected via an automated series of steps to analyze the network configuration of the remote network, optionally with input from the user.

[0071] In at least one embodiment, approved remote IP address(s) that will be allowed to access devices in the interior of the home network 102 are determined. During the implicit-authorization phase, in at least one embodiment, code on the access device 104 executes a process to determine the configuration of the remote network 108. From this remote-network information, the access device 104 can compute and then provide to the home router 106 the remote IP address (or multiple addresses) that will be allowed to access the home network 102.

[0072] First, note that there are different types of IP addressing schemes used today. For most home networks, a single public IP address is used and assigned to the home router. Devices “behind” this router—that is, in the interior of the home network—typically have “private” or “non-routable” IP addresses, which, for example, are provided to devices for a short span of time via Dynamic Host Configuration Protocol (DHCP). Connections from such devices will appear to have the public IP address of the home router, due to Network Address Translation (NAT). Other networks, such as corporate or educational networks, typically have routable, public IP addresses, and their networks will typically be structured as multiple individual subnets.

[0073] In at least one embodiment, to determine the range of IP addresses that constitute the remote network 108, and which should be allowed to access the user’s device(s) in their home network 102, the access device 104 determines the access-device IP address on the remote network 108. In at least one embodiment, the access device 104 is configured to perform a set of functions if the access device 104 determines that the access-device IP address on the remote network 108 is a private address and is configured to perform a different set of functions if the access device determines that the access-device IP on the remote network 108 is a public address.

[0074] In at least one embodiment, the access-device IP address is a private address. The access device determines that it is behind a NAT router, and in such a scenario, any other devices on that (remote) network will appear to have the same IP address as that router were they to access the user’s home network. In this embodiment, the access device declares that the IP address in use by the router should be considered allowable for connections to the home network. This permits any devices on the interior of that remote network 108 access to the home.
In at least one embodiment, the access-device IP address is a public address. The access device determines that it is on a network made up of other public IP addresses. Typically these are large corporate networks, and it may not be desirable to allow all devices on such a large network access into the home. The access device determines the current subnet mask of the remote network, which indicates the range of IP addresses that are a part of the nearby network. Typically this will indicate the range of IP addresses for a given department, or site, in an enterprise. This process provides a more restricted range of IP addresses that are allowed to access the home network, based on the internal structure of the remote network.

FIG. 2 is a flowchart depicting an exemplary embodiment of this process of determining remote network configuration parameters.

At 202, the access-device IP address on the remote network is determined. For example, the access-device 104 may be configured to determine its own IP address.

At 204, the access-device IP address is determined to be public or private. In at least one embodiment, to determine whether the access-device IP address is private or public, the access-device IP address is compared to one or more predetermined sets of IP addresses. These one or more predetermined sets of IP addresses may represent one or more ranges used for standard private IP addressing. For example, if the IP address is in the range 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255, or 192.168.0.0 – 192.168.255.255, then the IP address is private, otherwise the IP address is public.

If the access-device IP address is private, then at 206 the WAN IP address of the remote router is determined. For example, the access-device may be configured to determine the WAN IP address of the remote router. At 208, this WAN IP address is used as a valid remote source address.

If the access-device IP address is public, then at 210 a subnet mask of the remote network is determined. For example, the access-device may be configured to determine the subnet mask of the remote network. At 212, the range of IP address(es) that are valid within that subnet are determined. For example, the access-device may be configured to determine the range of IP address(es) that are valid within that subnet. At 214, this range of IP addresses are used as valid remote source addresses.

Example 1 (Private Addressing): As an exemplary embodiment, suppose that the user initiates the implicit authorization process on a neighbor’s home network, perhaps to allow that neighbor to access a home security camera while the owner is away. Home networks are typically built with NAT routers and private IP addresses. In at least one embodiment, the access device determines that the access-device IP address on this remote network is 192.168.1.200, and is thus
a private address. Since private addressing is in use, any device on that remote network that attempts to access the original home network will appear to be coming from the WAN IP address of the router, due to Network Address Translation (NAT). This means that the access device’s private address cannot itself be used to configure access to the home network.

[0082] In at least one embodiment, the access device determines the WAN IP address of its current router (using ICMP protocols, such as via ping –r), and securely transmits this to the home router. In an exemplary embodiment, the access device determines the remote router’s WAN IP address to be 130.207.14.1, and will use this as the approved remote IP address.

[0083] Example 2 (Public Addressing): Suppose in this exemplary embodiment that the user initiates the implicit authorization process on a network with public addressing. This will typically be a corporate or university network. In at least one embodiment, the access device determines that the access-device IP address on this network is 128.61.31.11, which is not in one of the standardized ranges for private addresses; thus, it is a public, routable IP address. Now, the access device could use this address as the approved remote IP address. This would mean, however, that only the access device itself could access services in the interior of the home network (since the access devices is the only client on the remote network with this particular IP address). The access device may mark all or, perhaps, a subset of the IP addresses on the remote network as approved for access to the home network.

[0084] In at least one embodiment, the access device 104 determines the subnet mask of the remote network 108. The subnet mask is generally used to partition large networks into subnetworks, such as by department or lab; it indicates which portion of an IP address is the network prefix, and which part is the host number. IP addresses with the same network prefix are considered to be on the same subnetwork. In this embodiment, the subnet mask is set to 255.255.240.0, which indicates that the network prefix is 128.61.16.0/20, and thus the set of IP addresses that are a part of this subnetwork are 128.61.16.1 up through 128.61.31.254. This range (represented either using so-called CIDR notation as 128.61.16.0/20 or as the range 128.61.16.1-128.61.31.254) is then securely transmitted to the home router 106. In at least one embodiment, this information is presented to users for verification. For example, one or more IP addresses in the range and/or the set of IP addresses that are part of the subnetwork (e.g., determined from the subnet mask) are presented to the user via a user interface of the access device.

[0085] Rather than simply presenting IP addresses and ranges, a reverse DNS lookup may be employed to render these details in a more readable form. In at least one embodiment, the access device is configured to perform a reverse DNS lookup and/or receive information resulting from a reverse DNS lookup. In an exemplary embodiment, if a user wishes to provision remote access
from her university lab to her home network, the access device can perform the steps above to produce the IP address range for her lab, and then the access device can perform a reverse DNS look up on that address to produce a human-readable network name. The access device may query the user with a request, such as, for example, “Allow access to your home from network hcilab.cc.gatech.edu?” In at least one embodiment, smaller and/or larger networks could additionally or alternatively be presented. For example, “Allow access from cc.gatech.edu, or all of gatech.edu?”

[0086] In at least one embodiment, the access device determines the specific set of devices that are allowed to be connected to by these addresses (at 142). In at least one embodiment, this information is collected via input from the user at the time the implicit authorization process is performed. For example, the access device 104 may present, via a user interface, one or more devices to which remote access may be granted, and/or the access device 104 may receive input from the user, via the user interface, corresponding to the one or more devices to which remote access is granted.

[0087] In some scenarios, determining the set of approved remote IP addresses may not be sufficient. In some scenarios, creating a mapping between approved remote addresses and the destination devices on the home network 102 that those remote addresses are allowed to connect to may be advantageous. In an exemplary embodiment, a user may not wish to provide the neighbors access to every device on the user’s home network 102, but the user may wish to restrict that access to only one or more particular devices, such as, for example, a security camera.

[0088] This process may use the device inventory database collected earlier, and transmitted to the access device 104 from the home router 106. The device inventory database is a list of all smart home devices, identified by a unique ID (such as a MAC address), complete with the device name and information about the ports on those devices that are open for receiving inbound connections.

[0089] The user may be involved in ascertaining which devices should be accessible from the remote network 108. In at least one embodiment, after the access device 104 collects the remote IP address information, the access device 104 presents a user interface to the user to allow the user to indicate which of the smart home devices should be accessible from the remote IP addresses. In at least one embodiment, the user can indicate which devices should be accessible, as well as optional policy settings such as the time duration for how long the access should be allowed. (An example user interface (UI) as well as discussion of optional policy settings are described in connection with FIG. 3.)
As noted, the user may be involved in specifying which devices back in the user’s home network 102 should be accessible from the given remote network (e.g., remote network 108). As an example, the app on the access device 104 may allow the user to select which devices will be permissible to connect to, during the implicit authorization phase. In at least one embodiment, the user interface allows the user to specify whether devices on the remote network should have access to all smart home devices. In at least one embodiment, the user interface allows the user to specify whether devices on the remote network should have access to only select devices on the home network. In at least one embodiment, the names of specific devices are retrieved from the device inventory information on the access device 104, which is received from the home router 106 and/or is periodically transmitted to the access device 104 from the home router 106.

In at least one embodiment, the access device 104 interacts with the user to possibly collect additional access policy information (at 144). This information may include, for example, a duration for which to allow access, or other parameters.

Since the user may have different preferences for how remote devices (e.g., other remote device 112) may connect into the home network 102, code on the access device 104 may also present a user interface at this point to collect additional policy information from the user. For example, the access device 104 may be configured to present a user interface for which a user may provide input regarding additional policy information and this user interface may be part of or separate from other user interfaces described herein. In at least one embodiment, this interface allows the user to indicate whether the current remote network should have permanent access to the smart home device (as may be the case for allowing access to a baby monitor from grandparents’ home network) or only transient access (such as when a user is accessing her baby monitor from a public WiFi network).

Additionally or alternatively, other optional configurations are possible. In at least one embodiment, the user requests the option to approve connection requests at the time they are made. This could allow, for instance, a notification to be securely delivered to the user’s phone each time an incoming connection attempt is made from a given remote network; the user can then approve or disapprove access to a given device at that time.

Once collected, in at least one embodiment, this information is transmitted to the home router 106 to provide a timeout value in its access control rules table.

In at least one embodiment, the access device 104 transmits new rule information back to the home router 106 (at 146). For example, from the remote network 108, the access device 104 may transmit the rule information to the router 106 via the public Internet 114.
In at least one embodiment, the router receives the rule information and updates the translation table and access rule databases accordingly (at 148, 150). In at least one embodiment, at this point, the home router 106 begins handling connection requests from remote networks in accordance with the new information provided to it by the access device 104.

In at least one embodiment, to initiate the implicit-authorization phase, the user simply brings the access device 104 into the remote network 108 from which the user desires to access the home and presses a “start” button. Of course, the user pressing a “start” button to initiate the implicit authorization phase is presented for exemplary purposes only and any feasible user input may be employed in one or more embodiments. In at least one embodiment, the access device 104 is configured to initiate the implicit authorization phase upon connection to the remote network 108.

FIG. 3 depicts an illustration of an example user interface 300 for allowing users to indicate access policies. In at least one embodiment, the system presents the user with a list of all current devices on the home network and allows the user to specify to which device(s) access is being provided. In the exemplary embodiment depicted in FIG. 3, the user interface 300 presents an example list 302 of devices currently on the home network for which access may be provided. The example list 302 includes Baby Cam, Home Security, and Nest Thermostat. In the depicted embodiment, the baby cam is selected as a device for which access is allowed and the home security and nest thermostat are not selected and therefore are not allowed access from the remote network. In the middle region 304 of the depicted user interface 300, the system indicates which remote network is being allowed access to the home. Finally, in the bottom region 306 of the depicted user interface 300, users can indicate any preferences for duration of access to be granted as well as whether the system should notify the user before granting access.

In at least one embodiment, at the end of the user interaction, code running on the access device 104 determines (1) the approved remote IP Address(s) that the user wishes to permit, (2) the allowable destination devices in the home network that these addresses are allowed to contact (named by the user, and associated with their unique IDs from the device inventory information). In one or more such embodiments, the access device 104 determines any additional policy information provided by the user, such as temporality of access, requirement for notifications, and so forth.

Once collected, in at least one embodiment, the access device 104 provides this information securely to the home router 106, using the security certificate information created during the set-up phase to encrypt and authenticate a connection to the home router using SSL or similar encrypted network connection. In at least one embodiment, both devices verify the identity
of the other via their certificates. The access device 104 then transmits the configuration parameters and policy information to the home router 106.

[0101] In at least one embodiment, the message sent from the access device 104 to the home router 106 is of a format similar to the following (and could be expressed in XML, JSON, or other representations):

```plaintext
ADD_TRANSLATION:
  Map_from: {remote_address="104.14.55.10",
            destination_port="2304"
  Map_to: {local_device_id="00:13:10:0F:BC:29",
           local_port="2304"}

ADD_TRANSLATION:
  Map_from: {remote_address_range="128.61.16.0/20",
            destination_port="80"
  Map_to: {local_device_id="00:25:9C:84:22:A9",
           local_port="80"}

ADD_ACCESS_RULE:
  IF SOURCE_ADDR == "104.14.55.10" AND
  DEST_PORT="2304" AND DATE () ≤ “December 7, 2015”
  THEN
    ALLOW
  ELSE
    DROP_CONNECTION

ADD_ACCESS_RULE:
  IF SOURCE_ADDR inRange(128.61.16.1,
                         128.61.31.254) AND DEST_PORT="80" THEN
    IF REQUEST_APPROVAL_FROM_USER ()
    == true THEN
      ALLOW
    ELSE
      DROP_CONNECTION
  ELSE
    DROP_CONNECTION
```

[0102] In at least one embodiment, the first two parts of the message add a new NAT translation, instructing the router 106 how to handle transit originating from the given remote addresses and intended for the specified ports. The router 106 is configured to use this information
to translate the inbound address of any connection requests from the home router 106’s IP address to the private address and port number on the interior of the network 102 and is configured to use this information to translate the source address of any outgoing communication from the private address of the smart home device 110 to the home router 106’s WAN address.

[0103] In at least one embodiment, the second two parts of the message configure the access rules (which may be considered the router’s firewall) to only allow inbound connections from the specified remote IP addresses, or address ranges, when attempting to connect to the specified ports. Shown in the second two parts of the message are example clauses that reflect user policy decisions made after collecting preferences from the user (e.g., at the time of implicit authorization). In the first rule, the user has specified that the access will only be allowed until a specified time (e.g., through December 7, 2015), and so the access rule reflects this timeout period. In the second rule, the user has requested notifications when access is attempted. In at least one embodiment, the function REQUEST_APPROVAL_FROM_USER ( ), when executed in the router, will generate a real-time notification to the user, which may be affirmed before access is permitted.

[0104] Once the message is received, the home router 106 updates its translation table database and its access rule database to include the new rules transmitted from the access device 104 and begins processing connection attempts in accordance with these rules. In at least one embodiment, the home router 106 is configured to allow access from the remote network(s) specified by the access device 104, for the time period requested by the user. After this, devices on this remote network are able to freely connect to the indicated smart home device. In at least one embodiment, other devices, from non-approved remote networks, are always denied the ability to connect by the home router 106.

[0105] In the above example messages, local devices are identified by a unique ID which is their MAC address. Other unique identifiers could be used, but in some scenarios the MAC address is the easiest to support.

[0106] After the user has authorized a remote network to permit access to a specific set of home devices, in at least one embodiment, the router is now configured to reject all other accesses, while permitting (and correctly translating) inbound traffic from the approved networks. In at least one embodiment, the access device does not need to remain resident in the remote network in order for this to occur. In at least one embodiment, the router 106 evaluates each attempted connection against its access rule database. Afterwards, the translation rules database may be used to rewrite incoming packets so that they are correctly delivered to example smart home device 110.

[0107] FIG. 1C is a flow diagram illustrating an overview of data flow and/or data processing by an example router of inbound and outbound traffic, in accordance with at least one embodiment.
In at least one embodiment, the inbound and outbound traffic depicted in FIG. 1C occur after the set-up phase and the implicit authorization phase.

In the depicted embodiment, the other remote device 112 is on the remote network 108.

In at least one embodiment, when a device (e.g., the other remote device 112) on a remote network (e.g., the remote network 108) attempts to connect to a device (e.g., smart home device 110) on the home network (e.g., the home network 102), the device initiates a TCP/IP connection request (e.g., via a SYN packet), which contains its source IP address and port number and contains the destination IP address and port number. The connection request may be transmitted from the other remote device 112 to the home router 106 via the public Internet 114 (at 152).

When this packet arrives at the home router 106, in at least one embodiment, the router 106 evaluates the rules in its access rules database, for example, to determine if the combination of source IP address and destination port number is permitted (at 154). If not, the connection request is silently dropped, and the remote device cannot connect.

If the rules in the access rules database do allow connection attempts from the given source address/destination port pair, then the router 106 retrieves relevant translation rules from its translation table database (at 156). In at least one embodiment, these rules specify how to rewrite both inbound and outbound packet headers so that traffic can transmit the home router 106 correctly. To do this, in at least one embodiment, the router 106 examines the destination port number contained in the packet and uses this as an index into its translation table database. The database contains mappings from port numbers to the link-layer address of the device 112 on the home network 102 that should receive packets received at that port number. Because IP addresses of devices on the home network may change over time, for example, due to DHCP and other common home protocols, in at least one embodiment, link-layer addresses are maintained in the translation table and/or are used for mapping to port numbers. From this link-layer address, the currently valid IP address for the home device 110 is then looked up.

At this point, in at least one embodiment, the router 106 rewrites the inbound packet, replacing the original destination IP address (which will be the router’s WAN IP address) with the local device IP address (at 158). The packet is then forwarded on to the local device 110 (at 160). The smart home device 110 then accepts the connection (at 162).

FIG. 4A is a flow diagram illustrating the flow and/or processing of example inbound traffic by an example router, in accordance with at least one embodiment. The remote device 412 attempts to establish a TCP connection by sending a request including a source address =
104.14.55.10, source port = 2978, a destination address = 130.207.14.1, and a destination port = 2304 (at 420).

[0114] The home router 406, which (in this example) has a WAN IP address of 130.207.14.1, receives the request and analyzes at least some of the information provided in the request with respect to at least some of the access rules from the access rules database (at 425). For example, the home router 406 determines if the example source-address, destination-port combination is one that is allowed according to the access rules.

[0115] In this example, the combination is allowed, so translation rule(s) are retrieved from the translation table database (at 430). The example translation table indicates that port 2304 is mapped to link-layer address 00:13:10:OF:BC:29. The local IP address corresponding to this link-layer address is determined to be 129.168.2.55.

[0116] The incoming packet may then be rewritten (at 435). For example, the home router 406 may be configured to replace the WAN IP address 130.207.14.1 with the local IP address 129.168.2.55.

[0117] After the incoming packet is rewritten, the packet may be forwarded to the smart home device (at 440). For example, the home router 406 may be configured to forward the written packet to the smart home device 410, which in this example, is the Nest Thermostat: Living Room.

[0118] The connection may then be accepted by the smart home device 410 (at 445).

[0119] Returning to FIG. 1C, outbound traffic may be handled similarly. In at least one embodiment, the translation table database is used to rewrite packets to have the correct source address as they transit the router 106.

[0120] In at least one embodiment, the home device 110 attempts to send a reply to the remote device 112 (at 164). The reply that is sent by the home device 110 may be received at the router 106, which then accesses the translation table database to be able to rewrite the packet with the appropriate information (at 166). For outbound traffic, the source IP address in the packet (which will be the private address of the smart home device 110) is rewritten to be the WAN address of the home router 106 (at 168). The packet is rewritten in such a way so that further responses from the remote device 112 are routed correctly. The router 106 then forwards this packet to the intended remote destination (at 170), which may be subsequently received by the remote device.

[0121] FIG. 4B is a flow diagram illustrating the flow and/or processing of outbound traffic by an example router, in accordance with at least one embodiment.
The smart home device 410 generates a reply to the remote device 412 (at 450). In this example, the source address is the smart home device 410 local IP address, and the destination address is the WAN IP address of the home router 406.

The reply is sent to and received by the home router 406. The home router 406 then retrieves the translation rules from the translation rule database (at 455).

After retrieving the corresponding translation rules, the outgoing packet is rewritten (at 460). In this example, the local source address 192.168.2.55 of the smart home device 410 is mapped to the WAN IP address 130.7.207.14.1 of the router 406.

The packet may then be forwarded to the remote device 412 by the home router 406 (at 465), and subsequently received by the remote device 412 (at 470).

Differences in Access Devices: In exemplary embodiments described herein, the access device is described as most commonly being a mobile phone. This is because the phone is a device that—due to its mobility—can be easily brought into a remote network, and is often with the user. But other devices (or even multiple devices) could be the access device in various different implementations. In at least one embodiment, if a user’s work computer is taken through the initial set-up process with the home router, it would be able to remotely provision access to the home network, even if the work computer’s IP address changes. In such at least one embodiment, this would allow easy remote access to the smart home devices from the work computer. In at least one embodiment, the original access device (the mobile phone) could delegate access to one or more specific devices.

Applicability to Standards: In at least one embodiment, the access device includes a separate application that the user runs to easily provision access. In at least one embodiment, this provisioning code is “baked in” to vendor’s remote access applications themselves, meaning that whenever they are run, they securely configure the user’s home router to allow access from the network the user is actually using at the moment. Access from other networks, in at least one embodiment, are always disallowed. Such an approach might be pursued as a standard that vendors would adopt.

Delegation: As currently described, in at least one embodiment, the access device is used each time a new remote network is provisioned. In some scenarios, this approach provides the greatest security for the home user. But there may be times when a householder wishes others to be able to provision access from new networks. In an exemplary embodiment, grandparents wish to have their own access device so that if they are traveling, or using a public WiFi network, they can still access the baby cameras of their grandchildren. In at least one embodiment, this
functionality is implemented by allowing delegation of access credentials, the householders can transmit special credentials to the grandparents’ phone or other device that can subsequently be used to configure new remote networks on their home router. In at least one embodiment, these delegated credentials allow access to a subset of smart home devices: for example, allowing the grandparents to set up new access to the baby cam, but not the home alarm system.

Revocation: In at least one embodiment, the system can also provide an easy way to monitor and even revoke access. Since the access device is able to securely communicate with the home router, in at least one embodiment, the access device requests a list of current access rules from the router and display these to the user, allowing viewing, editing and/or removal of access rights previously granted.

Additional User Policy Actions: As mentioned before, users may provide additional policy information about how connection attempts are to be handled. In at least one embodiment, notifications are used to request user input regarding connection attempts. In at least one embodiment, since the router has a secure connection to the access device (e.g., the user’s phone), the router optionally delivers notification when certain connections are attempted. This allows the user to, for instance, approve or disapprove each connection at the time it is made. Other, almost arbitrary, policy actions could also be included, dependent only on the code that runs on the router and the complexity of the UI on the access device. In an exemplary embodiment, options could be created to log traffic, perform deep packet analysis to permit certain content from flowing to the remote device, and so forth.

In this exemplary embodiment use case scenario, Steve will be going on a business trip to his company’s branch office in Chicago for two weeks and will be staying in a hotel while there. He also plans to visit his parents while there.

Steve has just installed a home security system and a baby camera. Before leaving, he downloads the Remote Access App for his iPhone, and uses the application to pair his phone with his home router via Bluetooth LE. The app notifies him that he is ready to configure the privacy and security of his devices at any time.

After arriving in Chicago, Steve checks into his hotel and connects to the hotel WiFi network. He initially tries to view the baby camera from his phone (e.g., via a baby-cam application), but access is denied. He can’t connect because the system is protecting all of his smart home devices from being accessed from any remote networks that haven’t been approved by him. He runs the Remote Access App, which determines the necessary network information for the hotel’s WiFi network, and then clicks “Allow.” He then goes back to the baby-cam application, which is now able to instantly connect back to the home network. Steve knows he’ll only be here
for two weeks, so he sets the Duration option of the Remote Access App to be for two weeks only. He also decides to allow access to his home security system while away so that he can check the alarm status while he travels.

[0134] The next day Steve goes to the company branch. His company laptop instantly joins the corporate network, but again, he cannot access the baby-cam from his laptop because all non-approved networks are blocked by default. To enable access, he pulls out his phone, and runs the Remote Access App, which again determines the network information of the company network. The Remote Access App defaults to the minimum allowed access, which is the specific department that Steve works in. Steve clicks approve on his phone, and is now able to view the baby cam from his laptop, since his laptop is on that same network (that is approved).

[0135] That weekend, Steve finally has time to visit his parents for an extended dinner. He tells them about the baby cam, and they’re excited to be able to see their new granddaughter. While visiting, Steve again brings up the Remote Access App, this time granting permanent access to the baby-cam from the grandparents’ network, meaning that they will be able to view their granddaughter securely any time they wish.

[0136] Because at least one embodiment of the exemplary systems and methods described herein includes a home router with additional functionality in its firmware (e.g., being able to communicate with the access device), any company that sells home networking equipment may be motivated to implement it. The system(s) and/or method(s) may be a “value add” to a home networking equipment provider, as it can be sold as a way to make their entire smart home more secure, without having to replace/update existing smart home devices, or for the router vendor to even have to partner with other home equipment vendors.

[0137] Internet Service Providers (ISPs) may also be motivated to adopt the systems and methods described herein for similar reasons. Most ISPs now typically rent home router/gateway boxes to their customers. A “smart home security” may allow ISPs to upcharge for additional functionality, which can then be pushed down into a software update for the gateway device.

[0138] In at least one embodiment, the application used on the access device does not need to be a standalone program. In at least one embodiment, the functionality for network configuration assessment and user policy gathering is integrated into other tools, such as ones provided by smart home equipment vendors or by ISPs and home networking equipment vendors. In an exemplary embodiment, Google’s OnHub router comes with an app called Google On that is used to control a router. The security functionality described herein could be readily integrated into such a tool. As incidents of smart home security compromises increase in the media, providing a
comprehensive security solution will become more desirable. Smart home equipment vendors will likely begin to tout their security features as a selling point.

[0139] FIG. 5 is a flow diagram illustrating access control to a local area network (LAN) from a wide area network (WAN), in accordance with at least one embodiment.

[0140] In at least one embodiment, the gateway 506 is configured to send a gateway LAN-access secret to the mobile device 504 (at 520). In at least one embodiment, the gateway 506 is configured to send the gateway LAN-access secret to the mobile device 504 while the mobile device 504 is connected to the home network 502.

[0141] In at least one embodiment, the mobile device 504 is configured to send, to the gateway 506, remote-access information that includes authentication information and an IP-range (at 530). In at least one embodiment, the authentication information is derived from the gateway LAN-access secret. In at least one embodiment, the IP-address range of one or more IP addresses associated with the mobile device is determined. In at least one embodiment, the mobile device 504 sends the remote-access information via the WAN while on the remote network 508. The mobile device 504 may have connected to the remote network 508, for example, after receiving the gateway LAN-access secret from the gateway 506 while the mobile device 504 was on the LAN side of the gateway 506.

[0142] In at least one embodiment, the gateway 506 maintains a whitelist of IP addresses that are allowed to connect to the home network 502. In at least one embodiment, after the gateway 506 sends the gateway LAN-access secret to the mobile device 504, the gateway 506 is configured to only allow traffic from the WAN to the LAN from IP addresses on the whitelist (at 540).

[0143] In at least one embodiment, the gateway 506 is configured to verify the authentication information (at 550.).

[0144] In at least one embodiment, the gateway 506 is configured to add the IP-range to the whitelist (at 560). After the IP-range is added to the whitelist, the gateway 506 may permit traffic from the IP addresses in the range to enter the home network 502.

[0145] FIG. 6 depicts an example method of controlling access to a local area network (LAN) from a wide area network (WAN), in accordance with at least one embodiment. In at least one embodiment, the method is carried out by a gateway that resides between the LAN and the WAN. In at least one embodiment, the gateway is the home router 106.

[0146] In block 602, the gateway sends a gateway LAN-access secret to a mobile device via a first-local communication path that does not include the WAN. For example, the gateway may generate a gateway LAN-access secret and/or may provide the generated gateway LAN-access
secret to the mobile device via a local-communication path. In at least one embodiment, the gateway LAN-access secret includes a gateway LAN-access certificate.

[0147] In at least one embodiment, the gateway receives a mobile-device LAN-access secret from the mobile device via a second local-communication path. For example, the mobile device may generate a mobile-device LAN-access secret and/or may provide the generated mobile-device LAN-access secret to the gateway via a local-communication path. In at least one embodiment, the mobile-device LAN-access secret includes a mobile-device LAN-access certificate.

[0148] In at least one embodiment, the first and second local-communication paths are the same local-communication paths.

[0149] In at least one embodiment, one or both of the first and second local-communication paths include the LAN.

[0150] In block 604, after the gateway sends the gateway LAN-access secret, the gateway only allows traffic from the WAN to the LAN from IP addresses on a whitelist maintained by the gateway. In at least one embodiment, the gateway was configured to only allow traffic from the WAN to the LAN from IP addresses on the whitelist prior to the gateway sending the gateway LAN-access secret. In at least one embodiment, the gateway was not configured to only allow traffic from the WAN to the LAN from IP addresses on the whitelist prior to the gateway sending the gateway LAN-access secret.

[0151] In block 606, the gateway receives remote-access information from the mobile device via the WAN. In at least one embodiment, the remote-access information includes authentication information derived from the gateway LAN-access secret and includes an IP-address range of one or more IP addresses associated with the mobile device. In at least one embodiment, the remote-access information further includes port-specific information associated with at least one IP address in the IP-address range. In at least one embodiment, the remote-access information further includes temporal-limitation information associated with at least one IP address in the IP-address range. In at least one embodiment, the remote-access information further includes LAN-device-limitation information associated with at least one IP address in the IP-address range. In at least one embodiment, the gateway receives the remote-access information at a port of the gateway that is unaffected by the whitelist.

[0152] In block 608, the gateway verifies the authentication information and responsively adds the IP-address range to the whitelist.
In at least one embodiment, the gateway collects LAN-device information regarding one or more devices on the LAN and transmits at least some of the collected LAN-device information to the mobile device.

One embodiment takes the form of a method of controlling access from an access device on a WAN to a LAN by a gateway connected to the WAN and LAN, that includes (a) sending, to the access device (not via the WAN), a gateway certificate for access to the LAN from the WAN, (b) receiving, from the access device (not via the WAN), an access device certificate, (c) receiving, from the access device, via the WAN: (i) information derived from [the gateway certificate and the access device certificate], and (ii) information regarding an IP address associated with the access device; and responsive to [verification of] the received information derived from [the gateway certificate and the access device certificate], (iii) adding the IP address associated with the device to a list of allowable IP addresses, and (iv) allowing [future] traffic from the IP address from the WAN to the LAN.

In at least one embodiment, the gateway certificate for access to the LAN is sent via one of Bluetooth, USB file copy, etc.

A second embodiment takes the form of a method of authenticating access device from remote network to home-network, that includes (a) associating an access device with a home router by exchanging keys, and (b) determining an IP address from which an access device try to get access comprising (i) if the IP address is private, determine IP address of router and provide router IP address as “allowable” remote connection origination and (ii) if the IP address is public, determine subnet mask, Compute range of IP addresses valid within that subnet, and Provide subnet IP addresses as “allowable” remote connection originations, wherein (i) Authenticating can be applied only to certain time frame/ certain device/ certain subdomain of subnet mask and (ii) the access device can delegate access to other device on the same network from which remotely accessing to home-network.

One embodiment takes the form of a method that includes generating a shared-secret certificate with an access device. The method also includes sending a device-inventory table to the access device. The method also includes receiving a permissions list based on the device-inventory table from the access device. The method also includes validating the permissions list based on the shared-secret certificate. The method also includes allowing remote access to at least one home device based on the validated permissions list.

Another embodiment takes the form of a system comprising a networked security system, a processor and a non-transitory computer-readable medium storing instructions operative,
when executed by the processor, to perform functions including at least those listed in the preceding paragraph.

[0159] In at least one embodiment, generating the shared-secret certificate with the access device comprises: (i) generating a router-public key; (ii) sending the router-public key to the access device over a local area network; (iii) receiving an access-device-public key; (iv) bundling the router-public key and the access-device-public key into a router digital certificate; and (v) signing the router digital certificate.

[0160] In at least one embodiment, the device-inventory table comprises at least one home-device and at least one port associated with the home device. In at least one such embodiment, the device-inventory table further comprises: a translation-table database which is used to maintain information about how to translate IP header information and an access-rule database which contains security rules about which external IP addresses are allowed to connect.

[0161] In at least one embodiment, validating the permissions list based on the shared-secret certificate with the access device comprises validating a router digital certificate with an access-device digital certificate associated with the permissions list.

[0162] In at least one embodiment, allowing remote access to at least one home device based on the validated permissions list comprises adding at least one IP address associated with the validated permissions to a list of allowable IP addresses.

[0163] Another embodiment takes the form of a method including generating a shared-secret certificate with a home router. The method also includes receiving a device-inventory table from the home router. The method also includes determining at least one remote IP address for access to the home router. The method also includes generating a permissions list via a user interface based on the at least one remote IP address and the device-inventory table. The method also includes sending the permissions list to the home router using the shared-secret certificate for enabling remote access to at least one home device based on the permissions list.

[0164] Another embodiment takes the form of a system comprising a networked security system, a processor and a non-transitory computer-readable medium storing instructions operative, when executed by the processor, to perform functions including at least those listed in the preceding paragraph.

[0165] In at least one embodiment, generating the shared-secret certificate with the home router comprises: (i) generating a access-device-public key; (ii) sending the access-device-public key to the home router over a local area network; (iii) receiving a router-public key; (iv) bundling
the access-device-public key and the router-public key into an access-device digital certificate; and (v) signing the access-device digital certificate.

[0166] In at least one embodiment, the device-inventory table comprises at least one home-device and at least one port associated with the home device.

[0167] In at least one embodiment, determining at least one remote IP address for access to the home router comprises determining that an access device IP address is a private IP address. In at least one such embodiment, determining that the access device IP address is a private IP address comprises determining a gateway-router IP address associated with the private IP address.

[0168] In at least one embodiment, determining at least one remote IP address for access to the home router comprises determining that the access device IP address is a public IP address. In at least one such embodiment, determining at least one remote IP address for access to the home router further comprises determining a range of IP addresses based on a subnet mask of the public IP address.

[0169] In at least one embodiment, generating a permissions list via a user interface based on the at least one remote IP address and the device-inventory table comprises receiving via the user interface a selection of at least one home-device from a list of user-interface home devices. In at least one such embodiment, comprising receiving via the user interface home-device policy information for at least one selected home-device.

[0170] In at least one embodiment, sending the permissions list to the home router using the shared-secret certificate comprises transmitting (i) the shared-secret certificate, (ii) the at least one remote IP address, and (iii) an identifier of at least one home device to the home router.

[0171] Another embodiment takes the form of a method of controlling access to a local area network (LAN) from a wide area network (WAN). The method is carried out by a gateway that resides between the LAN and the WAN. The method includes sending a gateway LAN-access secret to a mobile device via a first local-communication path that does not include the WAN. The method also includes receiving a mobile-device LAN-access secret from the mobile device via a second local-communication path that does not include the WAN. The method also includes after sending the gateway LAN-access secret and receiving the mobile-device LAN-access secret, only allowing traffic from the WAN to the LAN from IP addresses on a whitelist maintained by the gateway. The method also includes receiving remote-access information from the mobile device via the WAN, wherein the remote-access information comprises (i) authentication information derived from the gateway LAN-access secret and the mobile-device LAN-access secret and (ii) an IP-address range of one or more IP addresses associated with the mobile device. The method also
includes the gateway verifying the authentication information and responsively adding the IP-address range to the whitelist.

[0172] In at least one embodiment, the first and second local-communication paths are the same local-communication path.

[0173] In at least one embodiment, the first and second local-communication paths are different local-communication paths.

[0174] In at least one embodiment, one or both of the first and second local-communication paths include the LAN.

[0175] In at least one embodiment, one or both of the first and second local-communication paths include a universal serial bus (USB) connection between the gateway and the mobile device.

[0176] In at least one embodiment, one or both of the first and second local-communication paths include a wireless connection between the gateway and the mobile device. In at least one such embodiment, the wireless connection includes a Bluetooth connection.

[0177] In at least one embodiment, the gateway LAN-access secret comprises a gateway LAN-access certificate.

[0178] In at least one embodiment, the mobile-device LAN-access secret comprises a mobile-device LAN-access certificate.

[0179] In at least one embodiment, the gateway was configured to only allow traffic from the WAN to the LAN from IP addresses on the whitelist prior to the gateway sending the gateway LAN-access secret and receiving the mobile-device LAN-access secret.

[0180] In at least one embodiment, the gateway was not configured to only allow traffic from the WAN to the LAN from IP addresses on the whitelist prior to the gateway sending the gateway LAN-access secret and receiving the mobile-device LAN-access secret.

[0181] In at least one embodiment, the remote-access information further comprises port-specific information associated with at least one IP address in the IP-address range.

[0182] In at least one embodiment, the remote-access information further comprises temporal-limitation information associated with at least one IP address in the IP-address range.

[0183] In at least one embodiment, the remote-access information further comprises LAN-device-limitation information associated with at least one IP address in the IP-address range.
In at least one embodiment, the method further includes collecting LAN-device information regarding one or more devices on the LAN and transmitting at least some of the collected LAN-device information to the mobile device.

Note that various hardware elements of one or more of the described embodiments are referred to as “modules” that carry out (i.e., perform, execute, and the like) various functions that are described herein in connection with the respective modules. As used herein, a module includes hardware (e.g., one or more processors, one or more microprocessors, one or more microcontrollers, one or more microchips, one or more application-specific integrated circuits (ASICs), one or more field programmable gate arrays (FPGAs), one or more memory devices) deemed suitable by those of skill in the relevant art for a given implementation. Each described module may also include instructions executable for carrying out the one or more functions described as being carried out by the respective module, and it is noted that those instructions could take the form of or include hardware (i.e., hardwired) instructions, firmware instructions, software instructions, and/or the like, and may be stored in any suitable non-transitory computer-readable medium or media, such as commonly referred to as RAM, ROM, etc.

Exemplary embodiments disclosed herein are implemented using one or more wired and/or wireless network nodes, such as a wireless transmit/receive unit (WTRU) or other network entity.

Although features and elements are described above in particular combinations, one of ordinary skill in the art will appreciate that each feature or element can be used alone or in any combination with the other features and elements. In addition, the methods described herein may be implemented in a computer program, software, or firmware incorporated in a computer-readable medium for execution by a computer or processor. Examples of computer-readable storage media include, but are not limited to, a read only memory (ROM), a random access memory (RAM), a register, cache memory, semiconductor memory devices, magnetic media such as internal hard disks and removable disks, magneto-optical media, and optical media such as CD-ROM disks, and digital versatile disks (DVDs). A processor in association with software may be used to implement a radio frequency transceiver for use in a WTRU, UE, terminal, base station, RNC, or any host computer.

FIG. 7 is a system diagram of an exemplary WTRU 702, which may be employed as an access device in embodiments described herein. As shown in FIG. 7, the WTRU 702 may include a processor 718, a communication interface 719 including a transceiver 720, a transmit/receive element 722, a speaker/microphone 724, a keypad 726, a display/touchpad 728, a non-removable memory 730, a removable memory 732, a power source 734, a global positioning
system (GPS) chipset 736, and sensors 738. It will be appreciated that the WTRU 702 may include any sub-combination of the foregoing elements while remaining consistent with an embodiment.

[0189] The processor 718 may be a general purpose processor, a special purpose processor, a conventional processor, a digital signal processor (DSP), a plurality of microprocessors, one or more microprocessors in association with a DSP core, a controller, a microcontroller, Application Specific Integrated Circuits (ASICs), Field Programmable Gate Array (FPGAs) circuits, any other type of integrated circuit (IC), a state machine, and the like. The processor 718 may perform signal coding, data processing, power control, input/output processing, and/or any other functionality that enables the WTRU 702 to operate in a wireless environment. The processor 718 may be coupled to the transceiver 720, which may be coupled to the transmit/receive element 722. While FIG. 7 depicts the processor 718 and the transceiver 720 as separate components, it will be appreciated that the processor 718 and the transceiver 720 may be integrated together in an electronic package or chip.

[0190] The transmit/receive element 722 may be configured to transmit signals to, or receive signals from, a base station over the air interface 716. For example, in one embodiment, the transmit/receive element 722 may be an antenna configured to transmit and/or receive RF signals. In another embodiment, the transmit/receive element 722 may be an emitter/detector configured to transmit and/or receive IR, UV, or visible light signals, as examples. In yet another embodiment, the transmit/receive element 722 may be configured to transmit and receive both RF and light signals. It will be appreciated that the transmit/receive element 722 may be configured to transmit and/or receive any combination of wireless signals.

[0191] In addition, although the transmit/receive element 722 is depicted in FIG. 7 as a single element, the WTRU 702 may include any number of transmit/receive elements 722. More specifically, the WTRU 702 may employ MIMO technology. Thus, in one embodiment, the WTRU 702 may include two or more transmit/receive elements 722 (e.g., multiple antennas) for transmitting and receiving wireless signals over the air interface 716.

[0192] The transceiver 720 may be configured to modulate the signals that are to be transmitted by the transmit/receive element 722 and to demodulate the signals that are received by the transmit/receive element 722. As noted above, the WTRU 702 may have multi-mode capabilities. Thus, the transceiver 720 may include multiple transceivers for enabling the WTRU 702 to communicate via multiple RATs, such as UTRA and IEEE 802.11, as examples.

[0193] The processor 718 of the WTRU 702 may be coupled to, and may receive user input data from, the speaker/microphone 724, the keypad 726, and/or the display/touchpad 728 (e.g., a liquid crystal display (LCD) display unit or organic light-emitting diode (OLED) display unit).
The processor 718 may also output user data to the speaker/microphone 724, the keypad 726, and/or the display/touchpad 728. In addition, the processor 718 may access information from, and store data in, any type of suitable memory, such as the non-removable memory 730 and/or the removable memory 732. The non-removable memory 730 may include random-access memory (RAM), read-only memory (ROM), a hard disk, or any other type of memory storage device. The removable memory 732 may include a subscriber identity module (SIM) card, a memory stick, a secure digital (SD) memory card, and the like. In other embodiments, the processor 718 may access information from, and store data in, memory that is not physically located on the WTRU 702, such as on a server or a home computer (not shown).

The processor 718 may receive power from the power source 734, and may be configured to distribute and/or control the power to the other components in the WTRU 702. The power source 734 may be any suitable device for powering the WTRU 702. As examples, the power source 734 may include one or more dry cell batteries (e.g., nickel-cadmium (NiCd), nickel-zinc (NiZn), nickel metal hydride (NiMH), lithium-ion (Li-ion), and the like), solar cells, fuel cells, and the like.

The processor 718 may also be coupled to the GPS chipset 736, which may be configured to provide location information (e.g., longitude and latitude) regarding the current location of the WTRU 702. In addition to, or in lieu of, the information from the GPS chipset 736, the WTRU 702 may receive location information over the air interface 716 from a base station and/or determine its location based on the timing of the signals being received from two or more nearby base stations. It will be appreciated that the WTRU 702 may acquire location information by way of any suitable location-determination method while remaining consistent with an embodiment.

The processor 718 may further be coupled to other peripherals 738, which may include one or more software and/or hardware modules that provide additional features, functionality and/or wired or wireless connectivity. For example, the peripherals 738 may include sensors such as an accelerometer, an e-compass, a satellite transceiver, a digital camera (for photographs or video), a universal serial bus (USB) port, a vibration device, a television transceiver, a hands free headset, a Bluetooth® module, a frequency modulated (FM) radio unit, a digital music player, a media player, a video game player module, an Internet browser, and the like.

FIG. 8 depicts an exemplary network entity 890 that may be used in embodiments of the present disclosure, for example as a home router. As depicted in FIG. 8, network entity 890 includes a communication interface 892, a processor 894, and non-transitory data storage 896, all of which are communicatively linked by a bus, network, or other communication path 898.
Communication interface 892 may include one or more wired communication interfaces and/or one or more wireless-communication interfaces. With respect to wired communication, communication interface 892 may include one or more interfaces such as Ethernet interfaces, as an example. With respect to wireless communication, communication interface 892 may include components such as one or more antennae, one or more transceivers/chipsets designed and configured for one or more types of wireless (e.g., LTE) communication, and/or any other components deemed suitable by those of skill in the relevant art. And further with respect to wireless communication, communication interface 892 may be equipped at a scale and with a configuration appropriate for acting on the network side—as opposed to the client side—of wireless communications (e.g., LTE communications, Wi-Fi communications, and the like). Thus, communication interface 892 may include the appropriate equipment and circuitry (perhaps including multiple transceivers) for serving multiple mobile stations, UEs, or other access terminals in a coverage area.

Processor 894 may include one or more processors of any type deemed suitable by those of skill in the relevant art, some examples including a general-purpose microprocessor and a dedicated DSP.

Data storage 896 may take the form of any non-transitory computer-readable medium or combination of such media, some examples including flash memory, read-only memory (ROM), and random-access memory (RAM) to name but a few, as any one or more types of non-transitory data storage deemed suitable by those of skill in the relevant art could be used. As depicted in FIG. 8, data storage 896 contains program instructions 897 executable by processor 894 for carrying out various combinations of the various network-entity functions described herein.
What is claimed is:

1. A method of controlling access to a local area network (LAN) from a wide area network (WAN), the method carried out by a gateway that resides between the LAN and the WAN, the method comprising:

   sending a gateway LAN-access secret to a mobile device via a first local-communication path that does not include the WAN;

   after sending the gateway LAN-access secret, only allowing traffic from the WAN to the LAN from IP addresses on a whitelist maintained by the gateway;

   receiving remote-access information from the mobile device via the WAN, wherein the remote-access information comprises (i) authentication information derived from the gateway LAN-access secret and (ii) an IP-address range of one or more IP addresses associated with the mobile device; and

   the gateway verifying the authentication information and responsively adding the IP-address range to the whitelist.

2. The method of claim 1 further comprising:

   receiving a mobile-device LAN-access secret from the mobile device via a second local-communication path that does not include the WAN,

   wherein the authentication information is further derived from the mobile-device LAN-access secret.

3. The method of claim 2, wherein the first and second local-communication paths are the same local-communication path.

4. The method of claim 2, wherein one or both of the first and second local-communication paths include the LAN.

5. The method of claim 2, wherein one or both of the first and second local-communication paths include a universal serial bus (USB) connection between the gateway and the mobile device or a wireless connection between the gateway and the mobile device.
6. The method of claim 2, wherein the mobile-device LAN-access secret comprises a mobile-device LAN-access certificate.

7. The method of claim 1, wherein the gateway LAN-access secret comprises a gateway LAN-access certificate.

8. The method of claim 1, wherein the gateway was configured to only allow traffic from the WAN to the LAN from IP addresses on the whitelist prior to the gateway sending the gateway LAN-access secret.

9. The method of claim 1, wherein the gateway was not configured to only allow traffic from the WAN to the LAN from IP addresses on the whitelist prior to the gateway sending the gateway LAN-access secret.

10. The method of claim 1, wherein the remote-access information further comprises port-specific information associated with at least one IP address in the IP-address range.

11. The method of claim 1, wherein the remote-access information further comprises temporal-limitation information associated with at least one IP address in the IP-address range.

12. The method of claim 1, wherein the remote-access information further comprises LAN-device-limitation information associated with at least one IP address in the IP-address range.

13. The method of claim 1, further comprising:

   collecting LAN-device information regarding one or more devices on the LAN; and

   transmitting at least some of the collected LAN-device information to the mobile device.

14. The method of claim 1, wherein receiving the remote-access information includes receiving the remote access information at a port of the gateway that is unaffected by the whitelist.

15. A system for controlling access to a local area network (LAN) from a wide area network (WAN), the system comprising:

   a gateway configured to reside between the LAN and the WAN;

   a processor, and
a non-transitory computer readable medium storing instructions operative, when executed by the processor, to perform functions including:

- sending a gateway LAN-access secret to a mobile device via a first local-communication path that does not include the WAN;

- after sending the gateway LAN-access secret, only allowing traffic from the WAN to the LAN from IP addresses on a whitelist maintained by the gateway;

- receiving remote-access information from the mobile device via the WAN, wherein the remote-access information comprises (i) authentication information derived from the gateway LAN-access secret and (ii) an IP-address range of one or more IP addresses associated with the mobile device; and

- the gateway verifying the authentication information and responsiveness adding the IP-address range to the whitelist.
DETERMINE ACCESS-DEVICE IP ADDRESS

IS ACCESS-DEVICE IP ADDRESS PUBLIC OR PRIVATE?

DETERMINE WAN IP ADDRESS OF REMOTE ROUTER

USE THIS ADDRESS AS A VALID REMOTE SOURCE ADDRESS

DETERMINE SUBNET MASK OF REMOTE NETWORK

COMPUTE RANGE OF IP ADDRESS(ES) VALID WITHIN THAT SUBNET

USE THIS RANGE AS VALID REMOTE SOURCE ADDRESSES

FIG. 2
Allow access to these devices:

- Baby Cam
- Home Security
- Nest Thermostat

From the remote network:

cc.gatech.edu

Send Approval Notification?

For duration:

- Forever
- One Day
- One Hour

ALLOW

FIG. 3
SEND GATEWAY LAN-ACCESS SECRET TO MOBILE DEVICE VIA LOCAL-COMMUNICATION PATH

ONLY ALLOW TRAFFIC FROM WAN TO LAN FROM IP ADDRESS(ES) ON WHITELIST

RECEIVE, FROM MOBILE DEVICE VIA WAN, REMOTE-ACCESS INFORMATION INCLUDING (I) AUTHENTICATION INFORMATION DERIVED FROM GATEWAY LAN-ACCESS SECRET AND (II) IP-ADDRESS RANGE OF IP ADDRESS(ES) ASSOCIATED WITH MOBILE DEVICE

VERIFY AUTHENTICATION INFORMATION AND RESPONSIVELY ADD IP-ADDRESS RANGE TO WHITELIST

FIG. 6
**INTERNATIONAL SEARCH REPORT**

**A. CLASSIFICATION OF SUBJECT MATTER**

INV. H04L29/06  H04L12/28

ADD.

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)

H04L

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

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

EPO-Internal, WPI Data

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>figure 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>figure 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>figure 7</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraph [0017]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraph [0019]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraph [0023]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraph [0027]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraph [0028]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraph [0032]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraph [0036]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraph [0037]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraph [0039]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraph [0042]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraph [0052]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraph [0066]</td>
<td></td>
</tr>
</tbody>
</table>

See patent family annex.

Further documents are listed in the continuation of Box C.

* 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

* "S" document member of the same patent family

Date of the actual completion of the international search

9 May 2017

Date of mailing of the international search report

19/05/2017

Name and mailing address of the ISA/

European Patent Office, P.B. 5018 Patentlaan 2
NL-2280 HV Rijswijk
Tel. (+31-70) 340-3040,
Fax: (+31-70) 340-3016

Authorized officer

Caragata, Daniel
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patent document cited in search report</td>
<td>Publication date</td>
<td>Patent family member(s)</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>EP 1821492 A1</td>
<td>22-08-2007</td>
<td>CN 101022383 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1821492 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 5175054 B2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2007221785 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KR 20070082209 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2007189321 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2015350893 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2015365933 A1</td>
</tr>
<tr>
<td>US 2010233960 A1</td>
<td>16-09-2010</td>
<td>CN 101841443 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE 102010011176 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 2230820 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GB 2468752 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2010220223 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2010233960 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 2010107565 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 4129783 B2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2004046430 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2004078573 A1</td>
</tr>
</tbody>
</table>