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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 December 2004 (16.12.2004)

PCT

(10) International Publication Number
WO 2004/110026 A1

(51) International Patent Classification[7]: H04L 29/06, 12/28

(21) International Application Number: PCT/US2004/017732

(22) International Filing Date: 4 June 2004 (04.06.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/476,364 5 June 2003 (05.06.2003) US

(71) Applicant *(for all designated States except US)*: **WIRELESS SECURITY CORPORATION** [US/US]; 643 Bair Island Road, Suite 305, Redwood City, CA 94063 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **WIEDMANN, Ulrich** [US/US]; 1204 Edgewood Road, Redwood City, CA 94062 (US). **LILLIE, Terrance L** [US/US]; 102 Vaqudlo Way, Redwood City, CA 94002 (US). **SNEIDERMAN, Richard P** [US/US]; 579 Fort Lasamic Drive, Sunnyvale, CA 94087 (US). **WIEDMANN, Christian** [US/US]; 163 Rutherford Ave., Redwood City, CA 94061 (US). **ZELJKO, Robert** [HR/US]; 3981 Will Rogers Drive, San Jose, CA 95117 (US).

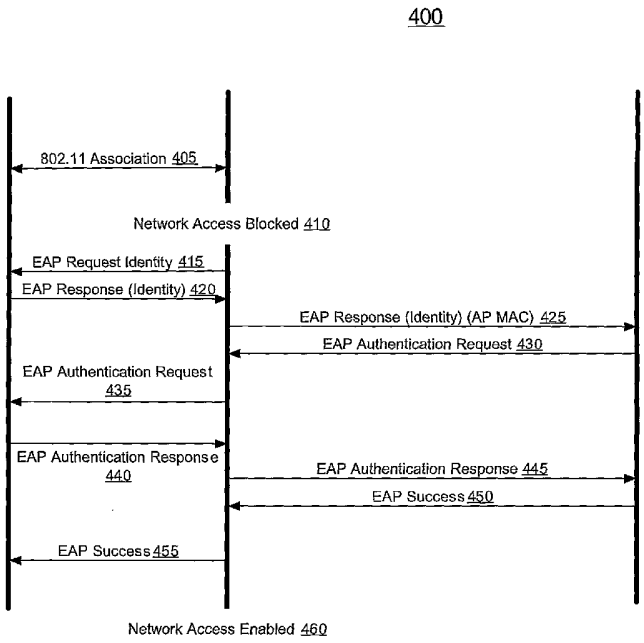
(74) Agent: **FAHMI, Tarek**; 12400 Wilshire Boulevard, Seventh Floor, Los Angeles, CA 90025-1030 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI,

[Continued on next page]

(54) Title: METHODS AND SYSTEMS OF REMOTE AUTHENTICATION FOR COMPUTER NETWORKS



(57) Abstract: As part of a network node (12) authentication process, a MAC address or other globally unique identifier of an access point (14) through which the network node (12) will access a computer network (10) is transmitted in an Extensible Authentication Protocol (EAP) or other authentication message to an authentication server (18) to uniquely identify the access point (14) to the authentication server (18).

WO 2004/110026 A1

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

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHODS AND SYSTEMS OF REMOTE AUTHENTICATION FOR COMPUTER NETWORKS

[0001] The present application is related to, incorporates by reference and claims the priority benefit of U.S. Provisional Application 60/476,364, entitled "METHODS AND SYSTEMS OF REMOTE AUTHENTICATION FOR COMPUTER NETWORKS", filed June 5, 2003.

FIELD OF THE INVENTION

[0002] The present invention relates to schemes for enhancing security within computer networks that include one or more wireless access points through the use of remote, secure authentication mechanisms.

BACKGROUND

[0003] Wireless local area networks (WLANs), such as those based on the IEEE 802.11a, 802.11b and 802.11g standards, are becoming ubiquitous in business, government and small office/home office (SOHO) settings because of the freedom afforded by and the decreasing costs of the underlying technology. Current security mechanisms for maintaining the confidentiality, integrity, and availability of wireless communications within such networks are, however, flawed. For example, although the above-cited IEEE standards specify both an authentication service and encryption protocol for wireless networks, methods for compromising these security measures have been well publicized. In response, the community of wireless network equipment developers and vendors has started to adopt the authentication procedures outlined in the 2001 IEEE 802.1x standard entitled "Port Based Network Access Control" in an effort to provide solutions to these security defects. The facilities needed to deploy such access

control measures, however, are both expensive and difficult for unsophisticated users to implement.

[0004] Before discussing the 802.1x access control mechanisms in detail, it is helpful to review some basics of WLANs in general. Unlike their wired LAN counterparts, WLANs provide for communication among network elements through wireless transmissions (e.g., radio transmissions), as opposed to wired, physical connections. **Figure 1** illustrates an exemplary prior art network 10 including a WLAN. In 802.11-based WLANs, clients or "stations" 12 (i.e., computers with wireless network interface cards (NICs)) interact with other network devices (printers, file servers, other clients, etc.) through access points (APs) 14, which act as bridges between the wired network 16 and wireless network 20. In some cases, wireless clients 12 may communicate directly with one another, without the use of APs.

[0005] The 802.1x standard does not itself specify any type of encryption procedures to be used within a network. To date, however, several equipment vendors have offered proprietary versions of dynamic key management for WLANs, using 802.1x as a delivery mechanism. In addition, the Wi-Fi Alliance (a non-profit industry consortium) has included 802.1x in its WPA security standard. Through dynamic key exchanges the authentication server 18 can return individual session keys to an AP 14 as part of the authentication process and these session keys can then be used for encrypted communications between the AP 14 and its clients 12. Dynamic key management provides a more secure environment than is typically found in an 802.11 WLAN because the use of multiple keys that are changed more frequently than is the case for a static key of an ordinary 802.11 network minimizes the opportunity for unauthorized users to uncover the keys.

[0006] Unfortunately, implementing an 802.1x solution for a WLAN is not an easy task. For example, the required network infrastructure is complex (potentially involving multiple authentication servers for use in cases of equipment failures) and expensive. In

addition, installing the necessary hardware and software in the network and nodes thereof generally cannot be undertaken by unsophisticated users. Consequently, deployment of 802.1x compliant WLANs has not yet become widespread at an enterprise level and is virtually nonexistent at a SOHO level.

SUMMARY OF THE INVENTION

[0007] Methods and apparatus for enhancing security within computer networks that include one or more wireless APs are described. In one embodiment, as part of a network node authentication process, access control parameters that define the network node's ability to access other resources (e.g., Internet resources) accessible through a computer network are exchanged by transmitting a MAC address (or other globally unique identifier) of an access point through which the network node will access the computer network in an exchange with a RADIUS or other authentications server (e.g., as part of an EAP message exchange with an authentication server) to identify the access point. In one particular embodiment, the MAC address of the access point is specified in a "Called-Station-ID" RADIUS protocol attribute.

[0008] The authentication process may make use of any such process, for example EAP TTLS, EAP TLS or PEAP. Alternatively, or in addition, the authentication process may require the network node and the authentication server (e.g., a RADIUS server) to identify themselves to one another using digital certificates and/or using a password. In other cases, the authentication process may provide for only the network node to be authenticated on the basis of a password. In various embodiments, the authentication process may make use of a secure channel, for example a channel that is both encrypted and integrity-protected, and may include an exchange of encryption keys for use between the access point and the network node.

[0009] The access control parameters may be selected from a list of possible rule sets during the authentication process. Such parameters may include rules for handling packets and/or may be associated with routines that allow the access point to monitor any

part of a packet header in a packet received from the network node. The access control parameters may be associated with state machines at the access point and/or may be assigned on a per-user basis. In some cases, the access control parameters are provided to the access point only upon successful verification of the network node's credentials by the authentication server.

[0010] The access point may include an access privilege table to which the access control parameters refer. In some embodiments the access point is a wireless network access point and the network node communicates with the access point using a wireless network communication protocol. In these and other embodiments, exchanging access control parameters may include transmitting a MAC address of the network node for authentication by the authentication server.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] A better understanding of the present invention can be obtained from the following detailed description in conjunction with the following drawings, in which:

[0012] **Figure 1** illustrates an exemplary prior art network including a WLAN;

[0013] **Figure 2** illustrates the basic authentication process in a typical network, according to one embodiment;

[0014] **Figure 3** illustrates an exemplary network having a wireless local area network configured for remote authentication, according to one embodiment of the present invention;

[0015] **Figure 4** illustrates an authentication process in a network, according to one embodiment of the present invention; and

[0016] **Figure 5** illustrates an exemplary computer architecture, according to one embodiment of the present invention.

DETAILED DESCRIPTION

[0017] Described herein are methods and apparatus for enhancing security within computer networks that include one or more wireless APs through the use of remote, secure authentication mechanisms. In some cases, the security enhancements may also be appropriate for wired networks.

[0018] In the following discussion, much of the information is described in terms of processes and procedures to be implemented by one or more computer systems executing appropriate algorithms which are embodiments of the present invention. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared and otherwise manipulated. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers or the like. It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise, it will be appreciated that throughout the description of the present invention, use of terms such as "processing", "computing", "calculating", "determining", "displaying" or the like, refer to the actions and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system's memories or registers or other such information storage, transmission or display devices. Moreover, as used herein, the term table can refer to any data structure.

[0019] As mentioned above, security in IEEE 802.11 networks is provided by an authentication service and an optional encryption protocol. The encryption protocol is known as WEP (wired equivalent privacy) and is a link-layer security protocol based on

the RC4 stream cipher, a symmetric cipher where the same key is used for both encryption and decryption. WEP was intended to provide confidentiality for wireless communications, through the use of encryption; access control for a network, through the option to discard improperly encrypted packets; and data integrity, through the use of a checksum. Unfortunately, however, WEP has been shown to have fundamental flaws (including flaws that allow hackers to uncover the actual cipher keys) which can be exploited to allow unauthorized clients to gain access to an 802.11 WLAN.

[0020] Likewise, the authentication process used in 802.11 WLANs is insecure. A client must authenticate and establish an association with an AP 14 prior to transmitting data. An association is simply a binding between the client 12 and an AP 14. The 802.11 standards provide for two types of authentication: open systems authentication and shared-key authentication.

[0021] Open systems authentication is usually the default mode of operation and allows any client 12 to associate with an AP 14 as long as the network identifiers (termed "SSID" or service set identification) used by the client 12 and the AP 14 match. Consequently, anyone who knows the SSID of a network can configure a client to be authenticated by an AP 14 on that network. Thus, because such SSIDs are broadcast by APs 14 in the clear as part of their beacon transmissions; open system authentication provides no security whatsoever.

[0022] Shared-key authentication is a one-way authentication mechanism used to provide more stringent access to network resources. The term "one-way" authentication is used because although the AP 14 must authenticate the client, there is no provision for a client to authenticate an AP 14. In a shared-key network a client 12 seeking to associate with an AP 14 must successfully encrypt a challenge string issued by the AP 14 before being authenticated. However, because it is the WEP key (and not a different authentication key) that is used in this process, shared-key authentication is really no more secure than WEP itself. Consequently, because WEP keys can be uncovered simply by monitoring

transmissions within a WLAN, shared-key authentication networks are also vulnerable to attack.

[0023] Recognizing these flaws in 802.11 WLANs, some AP equipment vendors have added an additional security layer in the form of an access control list based on client MAC addresses. In such cases, the AP 14 allows only those clients with authorized MAC addresses to create an association. However, such MAC-address filters are somewhat time consuming to establish and maintain and, consequently, are not often used.

[0024] Given the weakness of current 802.11 security mechanisms, some equipment vendors and network operators have begun to implement WLAN access control based on the relatively new IEEE 802.1x standard. The 802.1x standard provides mechanisms for client authentication, network access control, and cryptographic key management within any network (i.e., whether it is a wired or wireless LAN). These mechanisms are based upon an existing authentication protocol known as the Extensible Authentication Protocol (EAP), which is specified in various Internet Engineering Task Force (IETF) Requests For Comments (RFCs). In 802.1x parlance, clients 12 seek access to a network through an authenticator (usually an AP 14 in the case of a WLAN), which refers such requests to an authentication server 18. In practice, the authentication server 18 is usually a Remote Authentication Dial-In User Service (RADIUS) server, although RADIUS is not specifically required by the 802.1x standard. Only if the authentication server verifies the client's 12 identity will the AP 14 allow the client 12 to access other network resources.

[0025] What is needed therefore are mechanisms to allow for more widespread deployment of this technology to provide enhanced security for new and existing WLANs. As indicated above, the 802.1x specification provides a procedure for network client authentication. In the context of wireless networks, such authentication is performed via an AP 14 and an authentication server 18, usually a RADIUS server.

[0026] **Figure 2** illustrates the basic authentication process 200 in a typical network, according to one embodiment. As the diagram illustrates, the client 12 (called the supplicant in 802.1x terminology) first establishes an association with the AP 14 (the authenticator) using the conventional 802.11 procedures (205). At this point, however, the AP 14 prevents the client 12 from further accessing network resources until the client is authenticated (210). The authentication process begins with the AP 14 transmitting an EAP request for the client's identity (credentials) (215) and the client 12 providing a response (220). These messages are encapsulated within wireless LAN frames in a process referred to as EAP over LAN.

[0027] Thereafter, the EAP information provided by the client 12 is passed by the AP 14 to an authentication server (e.g., a RADIUS server) 18 over the wired LAN 16 (225). This time, the EAP information is encapsulated within a packet that conforms to the RADIUS protocol (a process known as EAP over RADIUS). The authentication server 18 then begins a dialog with the AP 14. The exact details of this exchange vary depending upon which authentication process is used in the network 10, but of importance to the present discussion is the need for the authentication server 18 to properly identify the AP 14 (230). The EAP authentication request is sent to the client 12 (235). The client 12 provides an EAP authentication response (240) to the AP 14. The AP 14 passes the authentication response to the authentication server 18 (245). Unless the AP 14 is properly identified, the authentication server 18 cannot process the authentication request. Assuming the AP 14 is properly identified (250), the authentication server 18 provides the information necessary to verify the client's identity (and in some cases, vice versa) (255), and the client 12 is granted access to the network via AP 14 (260).

[0028] Various authentication procedures which might be used in such an authentication scheme include EAP-TLS (transport level security), in which both the client and the authentication server identify themselves to one another using digital certificates; EAP-

TTLS (tunneled TLS), in which the client and authentication server identify themselves to one another but only the server has a digital certificate; EAP-SRP (secure remote password), in which both devices are authenticated using a password; EAP-MD5, in which only the client is authenticated by the server on the basis of a password; and protected EAP (PEAP), which uses a secure channel. In the EAP-TLS, EAP-TTLS and EAP-SRP processes, encryption keys for use between the AP 14 and the client 12 are generated as part of the exchange. In PEAP, a secure channel that is both encrypted and integrity-protected with TLS is created and then a new EAP negotiation with another EAP type occurs, authenticating the network access attempt of the client. Because the TLS channel protects EAP negotiation and authentication for the network access attempt, password-based authentication protocols that are normally susceptible to an offline dictionary attack can be used for authentication.

[0029] Regardless of the authentication method used, however, conventional authentication techniques employing RADIUS servers require that the AP 14 be identified using its Internet Protocol (IP) addresses. This IP address is used for a variety of reasons, most importantly to look up the shared secret that is used to protect communications between the AP 14 and the authentication server 18. Thus, the procedure cannot be used where AP IP addresses are subject to change, for example as would occur when the authentication server 18 is connected to private network 10 through a device which performs network address translation. An example of a situation in which an AP might have an IP address that is subject to change involves connecting the LAN 16 to the authentication server 18 via the Internet.

[0030] A RADIUS server generally is not connected to the private LAN directly since it may not be economically feasible for a network operator to do so. As mentioned above, deploying such a network is a costly and technically complex proposition. Therefore, it is an aspect of the present invention to provide a remote authentication mechanism for private LAN owners/operators that may be utilized on a fee for service or other basis. In

this model, LAN owners/operators are spared the cost of purchasing, installing and maintaining expensive server resources and instead may lease the authentication services from a third party provider.

[0031] **Figure 3** illustrates an exemplary network 320 having a wireless local area network configured for remote authentication, according to one embodiment of the present invention. According to this embodiment, the private LAN 316 is connected to the Internet 322 via a router 324. Router 324 may include a firewall application, or the firewall may be executing on a separate machine. The firewall acts as a filter that prevents unauthorized users from gaining access to private LAN 316 and its resources.

[0032] Connected between LAN 316 and the Internet 322, router 324 directs network traffic (i.e., packets) according to its programmed routing tables. As part of this process, router 324 usually performs network address translation (NAT), without which the multiple nodes of LAN 316 could not share the single address on the Internet 322. NAT of course involves the substitution of a LAN node's true IP address for a "masquerade" address provided by router 324, thus the IP address of AP 314 is hidden to outside resources (such as authentication server 318) and cannot serve as an effective identifier outside of LAN 316.

[0033] Other network configurations may involve APs 314 being assigned IP addresses dynamically. That is, a particular AP 314 may not identify itself using the same IP address each time it tries to provide a connection to a private network. This would represent another instance in which the use of an IP address to identify an AP 314 to the authentication server (whether remote or local to LAN 316) would be unsatisfactory.

[0034] In order to allow for these types of network configurations (i.e., the use of a remote authentication server 318 and/or networks in which APs 314 may be assigned different IP addresses from time to time), the present method and system involves utilizing an AP identifier other than an IP address in connection with the authentication process. Any AP parameter that remains unchanged may be used, however, in one

embodiment, an AP's MAC (media access controller) address, rather than its IP address is used in connection with such authentication. The MAC address is a parameter that is not affected by NAT when an AP 314 establishes a connection to the authentication server 318 via router 324. In other embodiments, other unique AP identifiers that could be passed unchanged from the AP 314 to the authentication server 318 as part of the authentication process may be used.

[0035] In order for the AP's MAC address to be passed from the AP 314 to the authentication server 318, the MAC address will need to be included in the EAP over RADIUS messages passed between these devices. The RADIUS protocol provides one or more existing fields within which such information may be provided. For example, the RADIUS protocol specifies a "Called-Station-ID" attribute, which was originally intended to identify the telephone number that a client was calling in order to establish a connection to a network. RADIUS was originally intended to support authentication of dial-up users, hence the need for such information. In the present context, however, this parameter is unnecessary and so the AP 314 could be modified to insert its MAC address in place of such a telephone number. Alternatively, other attributes of the RADIUS protocol that are otherwise unused in the authentication exchange between AP 314 and server 318 could be used for this purpose.

[0036] **Figure 4** illustrates an authentication process 400 in a network 320, according to one embodiment of the present invention. As the diagram illustrates, the client 312 first establishes an association with the AP 314 (the authenticator) using the conventional 802.11 procedures (405). At this point, however, the AP 314 prevents the client 312 from further accessing network resources until the client is authenticated (410). The authentication process begins with the AP 314 transmitting an EAP request for the client's identity (credentials) (415) and the client 312 providing a response (420). These messages are encapsulated within wireless LAN frames in a process referred to as EAP over LAN.

[0037] Thereafter, the EAP information provided by the client 312 is passed by the AP 314 to an authentication server (e.g., a RADIUS server) 318 over the wired LAN 316 (425). This time, the EAP information is encapsulated within a packet that conforms to the RADIUS protocol (a process known as EAP over RADIUS). The authentication server 318 then begins a dialog with the AP 314. The authentication server 318 is configured to initiate its authentication procedures using the AP's MAC address rather than the "masquerade" IP address provided by router 324. Once the AP 314 is identified on the basis of its MAC address (or other unique identifying parameter), the authentication server 318 may determine which LAN 316 is involved (e.g., via a table lookup to associate the AP MAC address with a particular LAN) and identify which authentication process to use for the client 312 that is now requesting access to that LAN. The authentication server 318 properly identifies the AP 314 (430) via its MAC address. The EAP authentication request is sent to the client 312 (435). The client 312 provides an EAP authentication response (440) to the AP 314. The AP 314 passes the authentication response to the authentication server 318 (445). Unless the AP 314 is properly identified, the authentication server 318 cannot process the authentication request. Assuming the AP 314 is properly identified (450), the authentication server 318 provides the information necessary to verify the client's identity (and in some cases, vice versa) (455), and the client 312 is granted access to the network via AP 314 (460).

[0038] In another embodiment, a software application executing on the client 312 may be configured to add the client's 312 and the AP's 314 MAC addresses to the username to be used for authentication. This way, the AP 314 does not need to be modified to add this information to a RADIUS field. Such a mechanism is useful for Aps 314 that support 802.1x but which do not pass MAC addresses for the AP 314 or the client 312 as part of the authentication message exchange.

[0039] Once the AP 314 is identified on the basis of its MAC address (or other unique identifying parameter), the authentication server 318 may determine which LAN 316 is

involved (e.g., via a table lookup to associate the AP MAC address with a particular LAN) and identify which authentication process to use for the client 312 that is now requesting access to that LAN. That is, different networks can employ different authentication procedures (e.g., EAP-TLS, EAP-TTLS, etc.) and through the table lookup or other association process the authentication server 318 can determine which procedure to employ for each network. If the client 312 is successfully identified according to its network's authentication procedure, the AP 314 is instructed to allow the client access to LAN 316.

[0040] As part of the authentication process, the authentication server 318 may provide session or dynamic keys for use between the AP 314 and a client 312. The use of dynamic keys (rather than a static WEP key for an entire network) helps to further enhance the security of the WLAN. Because such keys are typically used for a much briefer time than is the case for a static WEP key, it is less likely than an unauthorized person can uncover the key and hijack the network. In fact, because such keys are unknown to the actual users of network 320 (i.e., the keys are only known by the AP 314 and the client 312) the most pervasive form of hacking a network, social engineering, is completely unavailable to potential hijackers.

[0041] Having briefly described an exemplary network architecture 320 which employs various elements of the present invention, a computer system 500 representing exemplary clients 312, and/or servers (e.g., servers 318), in which elements of the present invention may be implemented will now be described with reference to **Figure 5**.

[0042] One embodiment of computer system 500 comprises a system bus 520 for communicating information, and a processor 510 coupled to bus 520 for processing information. Computer system 500 further comprises a random access memory (RAM) or other dynamic storage device 525 (referred to herein as main memory), coupled to bus 520 for storing information and instructions to be executed by processor 510. Main memory 525 also may be used for storing temporary variables or other intermediate

information during execution of instructions by processor 510. Computer system 500 also may include a read only memory (ROM) and/or other static storage device 526 coupled to bus 520 for storing static information and instructions used by processor 510.

[0043] A data storage device 527 such as a magnetic disk or optical disc and its corresponding drive may also be coupled to computer system 500 for storing information and instructions. Computer system 500 can also be coupled to a second I/O bus 550 via an I/O interface 530. Multiple I/O devices may be coupled to I/O bus 550, including a display device 543, an input device (e.g., an alphanumeric input device 542 and/or a cursor control device 541). For example, Internet information may be presented to the user on the display device 543.

[0044] The communication device 540 is for accessing other computers (servers or clients) via a network 316, 322. The communication device 540 may comprise a modem, a network interface card, or other well-known interface device, such as those used for coupling to Ethernet, token ring, or other types of networks.

[0045] Thus, methods and apparatus for enhancing security within computer networks that include one or more wireless APs have been described. It will be appreciated that the embodiments described above are cited by way of example, and that the present invention is not limited to what has been particularly shown and described hereinabove. Rather, the scope of the present invention includes both combinations and subcombinations of the various features described hereinabove, as well as variations and modifications thereof which would occur to persons skilled in the art upon reading the foregoing description and which are not disclosed in the prior art.

CLAIMS

We claim:

1. A method, comprising exchanging, as part of a network node authentication process, access control parameters that define the network node's ability to access other resources accessible through a computer network, wherein exchanging access control parameters includes transmitting a MAC address of an access point through which the network node will access the computer network in an authentication message to an authentication server to uniquely identify the access point to the authentication server.

2. The method of claim 1, wherein the authentication message comprises an EAP message.

3. The method of claim 1, wherein the network node authentication process makes use of an EAP TTLS authentication process.

4. The method of claim 1 wherein the network node authentication process makes use of an EAP TLS authentication process.

5. The method of claim 1 wherein the network node authentication process makes use of a PEAP authentication process.

6. The method of claim 1 wherein the network node authentication process includes the network node and the authentication server identifying themselves to one another using digital certificates.

7. The method of claim 1 wherein the network node authentication process requires the network node and the authentication server to be authenticated using a password.

8. The method of claim 1 wherein the network node authentication process provides for only the network node to be authenticated on the basis of a password.

9. The method of claim 1 wherein the network node authentication process uses a secure channel.

10. The method of claim 9 wherein the secure channel is both encrypted and integrity-protected.

11. The method of claim 1 wherein the network node authentication process includes an exchange of encryption keys for use between the access point and the network node.

12. The method of claim 1 wherein the authentication server comprises a RADIUS server.

13. The method of claim 1 wherein the access control parameters are selected from a list of possible rule sets during the authentication process.

14. The method of claim 1 wherein the access control parameters comprise rules for handling packets.

15. The method of claim 1 wherein the access control parameters are associated with routines that allow the access point to monitor any part of a packet header in a packet received from the network node.

16. The method of claim 1 wherein the access control parameters are associated with state machines at the access point.

17. The method of claim 1 wherein the access point includes an access privilege table to which the access control parameters refer.

18. The method of claim 1 wherein the access control parameters are assigned on a per-user basis.

19. The method of claim 1 wherein the resources include Internet access.

20. The method of claim 1 wherein the access control parameters are provided to the access point only upon successful verification of the network node's credentials by the authentication server.

21. The method of claim 1 wherein the access point comprises a wireless network access point and the network node communicates with the access point using a wireless network communication protocol.

22. The method of claim 1, wherein exchanging access control parameters further includes transmitting a MAC address of the network node for authentication by the authentication server.

23. The method of claim 1, wherein the MAC address of the access point is specified in a "Called-Station-ID" RADIUS protocol attribute.

24. A method, comprising exchanging, as part of a network node authentication process, a unique identifier other than an Internet protocol address of an access point through which the network node will access a computer network in an authentication message to an authentication server to uniquely identify the access point to the authentication server.

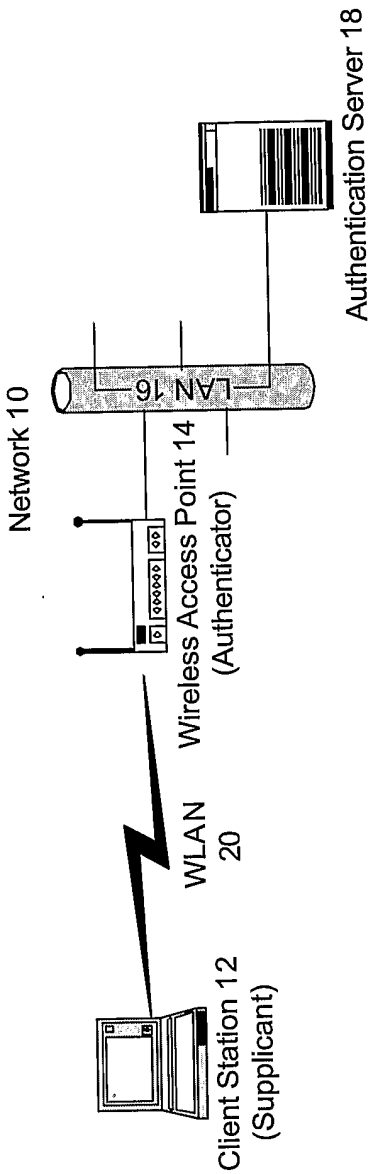


FIG. 1
(Prior Art)

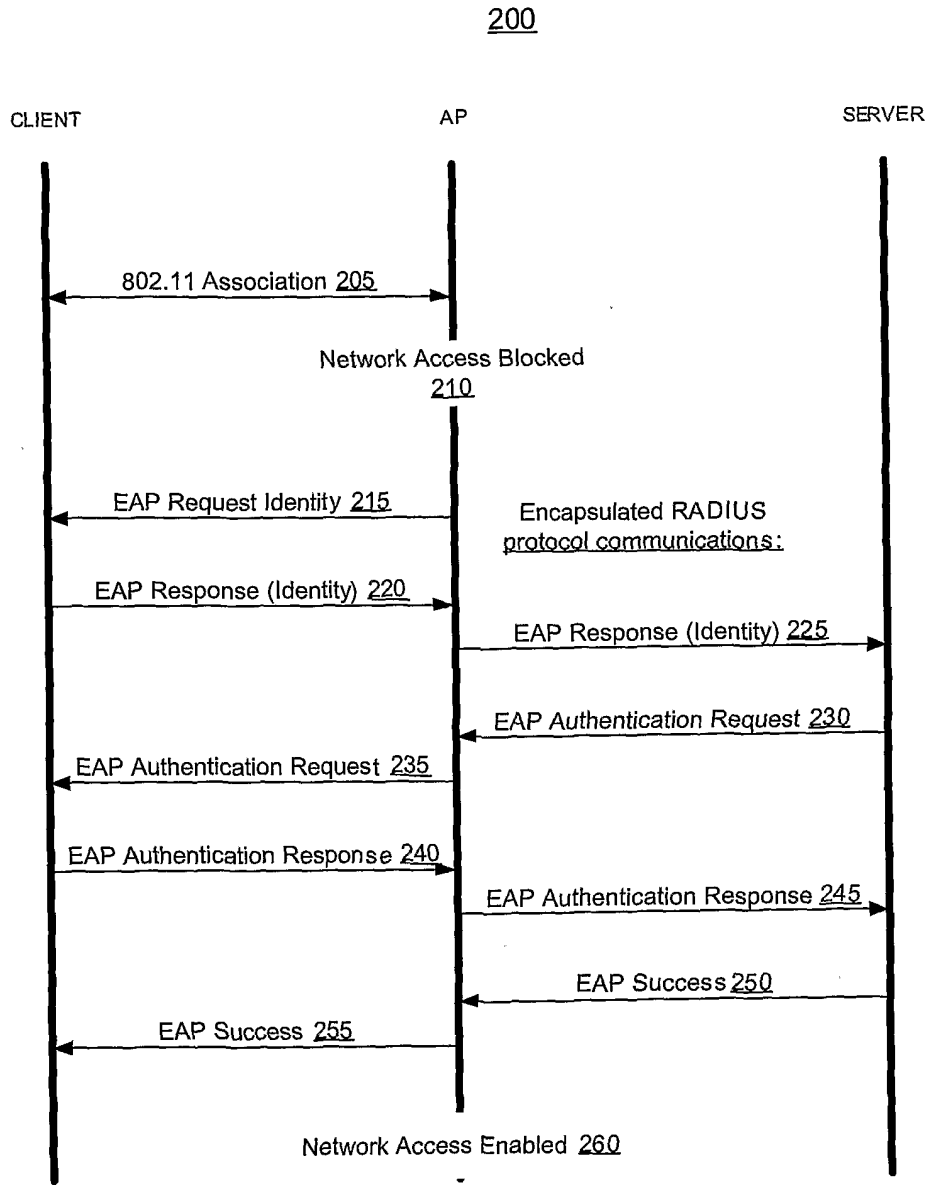

200
CLIENT
AP
SERVER
802.11 Association 205
Network Access Blocked 210
EAP Request Identity 215
Encapsulated RADIUS protocol communications:
EAP Response (Identity) 220
EAP Response (Identity) 225
EAP Authentication Request 230
EAP Authentication Request 235
EAP Authentication Response 240
EAP Authentication Response 245
EAP Success 250
EAP Success 255
Network Access Enabled 260

FIG. 2

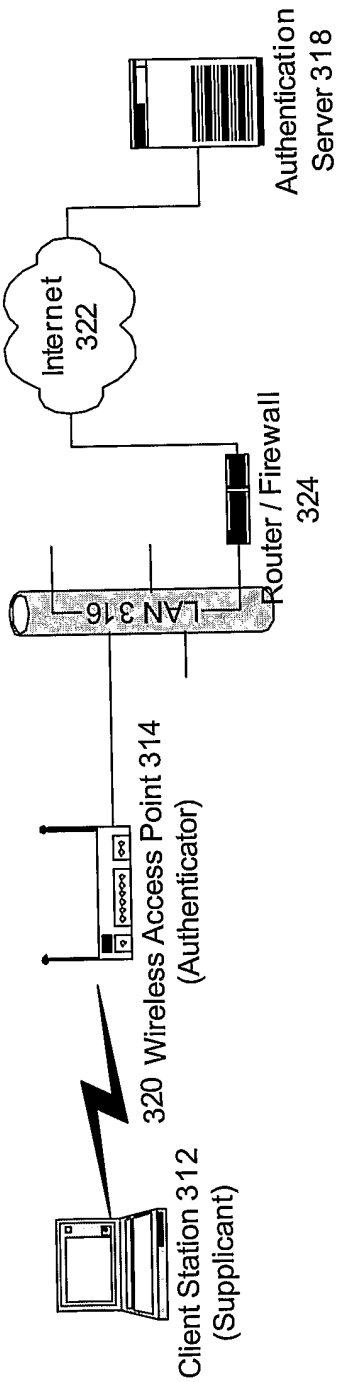

Authentication Server 318
Internet 322
Router / Firewall 324
LAN 316
320 Wireless Access Point 314 (Authenticator)
Client Station 312 (Supplicant)
300

FIG. 3

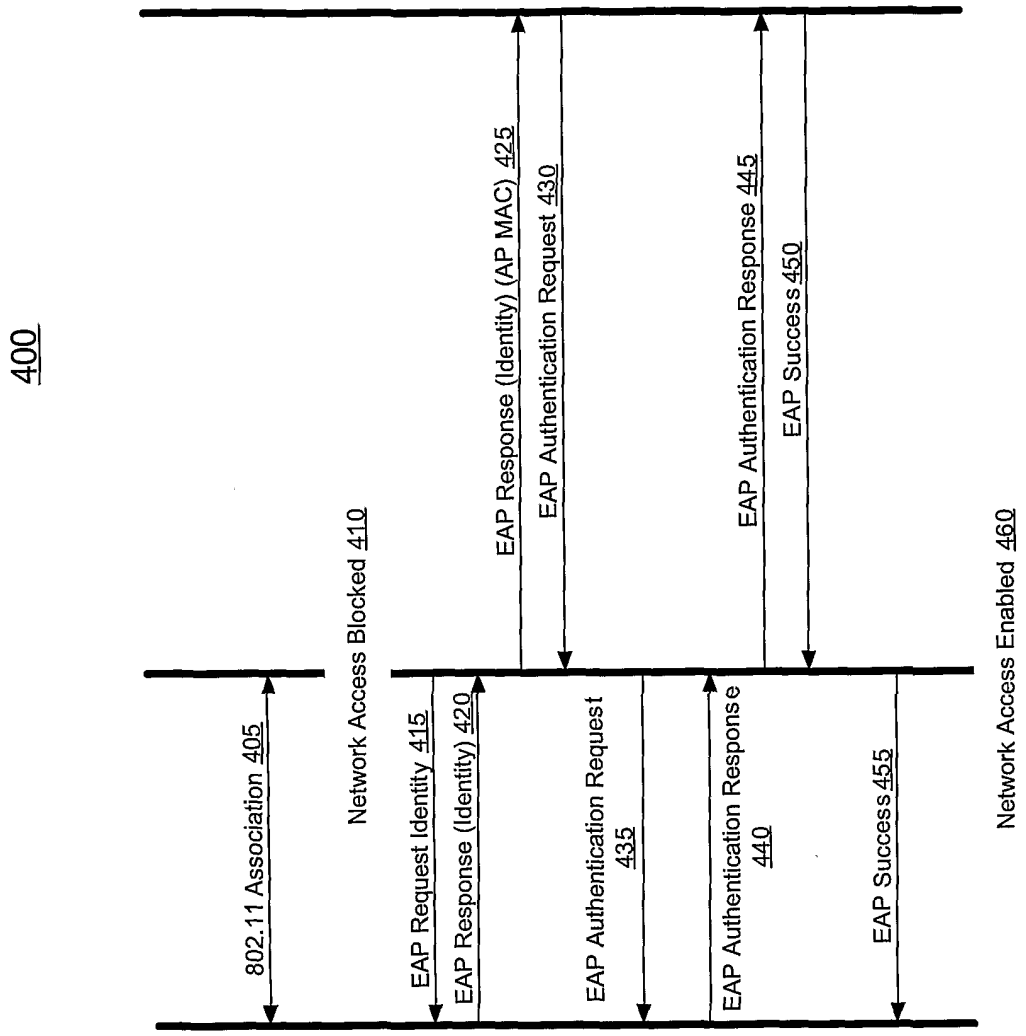

400
802.11 Association 405
Network Access Blocked 410
EAP Request Identity 415
EAP Response (Identity) 420
EAP Response (Identity) (AP MAC) 425
EAP Authentication Request 430
EAP Authentication Request 435
EAP Authentication Response 440
EAP Authentication Response 445
EAP Success 450
EAP Success 455
Network Access Enabled 460

FIG. 4

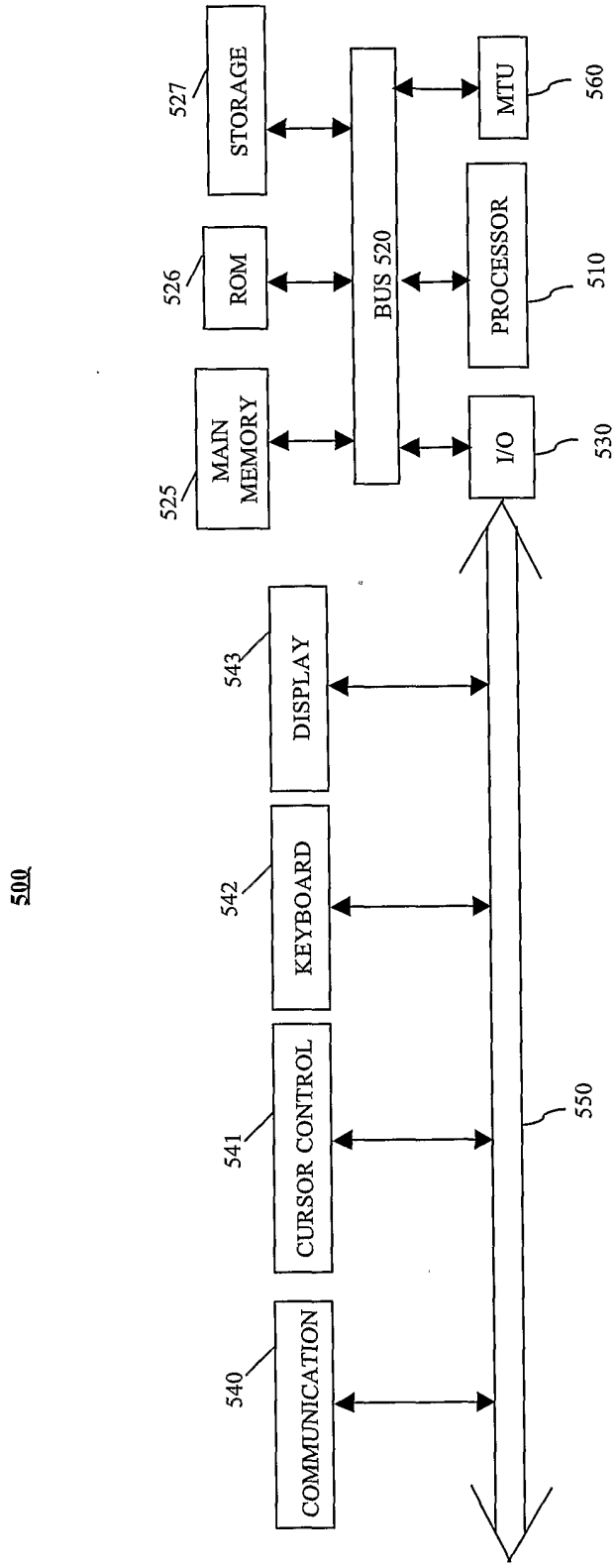

500
527
STORAGE
526
ROM
525
MAIN MEMORY
BUS 520
MTU
560
PROCESSOR
510
I/O
530
543
DISPLAY
542
KEYBOARD
541
CURSOR CONTROL
540
COMMUNICATION
550

FIG. 5

INTERNATIONAL SEARCH REPORT

International Application No
T/US2004/017732

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L12/28

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)
IPC 7 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 practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 081 895 A (INTEL CORP) 7 March 2001 (2001-03-07)	24
Y	paragraph '0011! paragraph '0013! - paragraph '0015! paragraph '0017! - paragraph '0022! figures 2,3A-3C	1-23
X	ABOBA B. ET AL: "RADIUS Support For Extensible Authentication Protocol (EAP)" INTERNET-DRAFT, 15 May 2003 (2003-05-15), XP015000024	24
Y	* section 1., first two paragraphs * * section 1.2 * * section 2.6.1. *	1-23

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 October 2004	27/10/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Homan, P

2

Form PCT/ISA/210 (second sheet) (January 2004)

International Application No
T/US2004/017732

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 03/029916 A (BLUESOCKET INC) 10 April 2003 (2003-04-10) paragraphs '0009!, '0011!, '0013! paragraph '0017! paragraph '0019! - paragraph '0021! paragraph '0064! figures 1A,1B	1-23

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
T/US2004/017732

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1081895 A	07-03-2001	EP 1081895 A1	07-03-2001
WO 03029916 A	10-04-2003	WO 03029916 A2	10-04-2003
		US 2003087629 A1	08-05-2003