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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 April 2003 (10.04.2003)

PCT

(10) International Publication Number
WO 03/030488 A1

(51) International Patent Classification[7]: H04L 29/06, H04Q 7/38

(21) International Application Number: PCT/FI02/00771

(22) International Filing Date:
27 September 2002 (27.09.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20011911 28 September 2001 (28.09.2001) FI

(71) Applicant *(for all designated States except US)*: **INTRASECURE NETWORKS OY** [FI/FI]; P.O. Box 38, FIN-02210 Espoo (FI).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **VAARALA, Sami** [FI/FI]; Neljäs Linja 22 A 24, FIN-00530 Helsinki (FI). **NUOPPONEN, Antti** [FI/FI]; Kaksoiskiventie 7-9 A 1, FIN-02760 Espoo (FI). **PIETIKÄINEN, Panu** [FI/FI]; Täysikuu 10 C 103, FIN-02210 Espoo (FI).

(74) Agent: **INNOPAT LTD**; P.O. Box 556, FIN-02151 Espoo (FI).

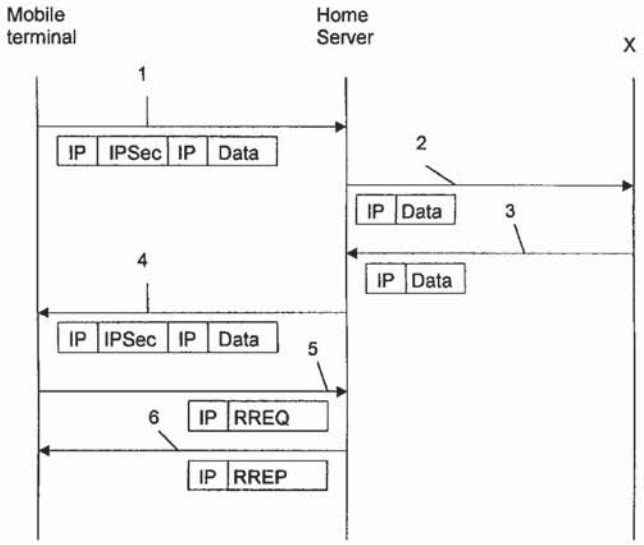
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT,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

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) **Title:** METHOD AND SYSTEM FOR ENSURING SECURE FORWARDING OF MESSAGES



(57) **Abstract:** The invention is concerned with a method for ensuring secure forwarding of a message is performed in a telecommunication network, comprising at least one terminal from which the message is sent and at least one other terminal to which the message is sent. In the method, one or more secure connections are established between different addresses of the first terminal and address of the ot her terminal, the connections defining at least said addresses of the two terminals. When the first terminal moves from one address to another adress, a secure connection, whose endpoints are the new address of the first terminal and the address of the other terminal, is registered to be at least one of the active connections.

WO 03/030488 A1

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.

METHOD AND SYSTEM FOR ENSURING SECURE FORWARDING OF MESSAGES

TECHNICAL FIELD

The method and system of the invention are intended to secure connections in telecommunication networks. Especially, the invention is meant to be used in wireless networks as a part of a mobile IP solution or an IPSec solution.

TECHNICAL BACKGROUND

An internetwork is a collection of individual networks connected with intermediate networking devices that function as a single large network. Different networks can be interconnected by routers and other networking devices to create an internetwork.

A local area network (LAN) is a data network that covers a relatively small geographic area. It typically connects workstations, personal computers, printers and other devices. A wide area network (WAN) is a data communication network that covers a relatively broad geographic area. Wide area networks (WANs) interconnect LANs across telephone networks and other media; thereby interconnecting geographically disposed users.

In fixed networks, there exist solutions to fill the need to protect data and resources from disclosure, to guarantee the authenticity of data, and to protect systems from network based attacks. IPSec is one such technology by means of which security is obtained.

The IP security protocols (IPSec) provides the capability to secure communications across a LAN, across private and public wide area networks (WANs) and across the internet. IPSec can be used in different ways, such as for building secure virtual private networks, to gain a secure access to a company network (as remote access IPSec

use), or to secure communication with other organisations, ensuring authentication and confidentiality and providing a key exchange mechanism. Even if some applications already have built in security protocols, the use of IPSec further enhances the security.

IPSec can encrypt and/or authenticate traffic at IP level. Traffic going in to a WAN is typically encrypted and/or authenticated and traffic coming from a WAN is decrypted and/or authenticated. IPSec is defined by certain documents, which contain rules for the IPSec architecture.

Two protocols are used to provide security at the IP layer; an authentication protocol designated by the header of the protocol, Authentication Header (AH), and a combined encryption/authentication protocol designated by the format of the packet for that protocol, Encapsulating Security Payload (ESP). Both AH and ESP are vehicles for access control based on the distribution of cryptographic keys and the management of traffic flows related to these security protocols.

Security association (SA) is a key concept in the authentication and the confidentiality mechanisms for IP. A security association is a one-way relationship between a sender and a receiver that offers security services to the traffic carried on it. If a secure two-way relationship is needed, then two security associations are required.

The term IPSec connection is used in what follows in place of an IPSec bundle of one or more security associations SAs, or a pair of IPSec bundles – one bundle for each direction – of one or more security associations. This term thus covers both unidirectional and bi-directional traffic protection. There is no implication of symmetry of the directions, i.e., the algorithms and IPSec transforms used for each direction may be different.

A security association is uniquely identified by three parameters. The first one, the Security Parameters Index (SPI), is a 32-bit string assigned to this SA. The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed. IP destination address is the second

parameter, which is the address of the destination end point of the SA, which may be an end user system or a network system such as a firewall or a router. The third parameter, the Security Protocol Identifier indicates whether the association is an AH or ESP security association.

Both AH and ESP support two modes used, transport and tunnel mode.

Transport mode provides protection primarily for upper layer protocols and extends to the payload of an IP packet. Typically, transport mode is used for end-to-end communication between two hosts. Transport mode may be used in conjunction with a tunnelling protocol (other than IPSec tunnelling).

Tunnel mode provides protection to the entire IP packet and is used for sending messages through more than two components. Tunnel mode is often used when one or both ends of a SA is a security gateway, such as a firewall or a router that implements IPSec. With tunnel mode, a number of hosts on networks behind firewalls may engage in secure communications without implementing IPSec. The unprotected packets generated by such hosts are tunnelled through external networks by tunnel mode SAs setup by the IPSec software in the firewall or secure router at boundary of the local network.

To achieve this, after the AH or ESP fields are added to the IP packet, the entire packet plus security fields are treated as the payload of a new outer IP packet with a new outer IP header. The entire original, or inner, packet travels through a tunnel from one point of an IP network to another: no routers along the way are able to examine the inner IP packet. Because the original packet is encapsulated, the new larger packet may have totally different source and destination addresses, adding to the security. In other words, the first step in protecting the packet using tunnel mode is to add a new IP header to the packet; thus the "IP|payload" packet becomes "IP|IP|payload". The next step is to secure the packet using ESP and/or AH. In case of ESP, the resulting packet is "IP|ESP|IP|payload". The whole inner packet is

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.