RTMP Is copy

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00, 9/08 | A1

(11) International Publication Number: WO 97/23972

(43) International Publication Date: 3 July 1997 (03.07.97)

(21) International Application Number: PCT/US96/19752

(22) International Filing Date: 20 December 1996 (20.12.96)

(30) Priority Data:
08/593,240 22 December 1995 (22.12.95) US

(71) Applicant: V-ONE CORPORATION [US/US]; Suite 302, 1803 Research Boulevard, Rockville, MD 10852 (US).

(72) Inventors: CHEN, James, F.; 9924 Hall Road, Potomac, MD 20854 (US). WANG, Jieh-Shan; 10903 Silent Wood Place, N., Potomac, MD 20878 (US).

(74) Agents: KENNEY, J., Ernest et al.; Bacon & Thomas, 4th floor, 625 Slaters Lane, Alexandria, VA 22314 (US).

(81) Designated States: CA, JP, KR, SG, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: APPLICATION LEVEL SECURITY SYSTEM AND METHOD

(57) Abstract

A system and method for establishing secured communications pathways across an open unsecured network, without compromising the security of any parties to the communication, involves establishing secured gateways or firewalls between the Internet and any party which desires protection by 1.) using a smart card to distribute shared secret keys between a computer which serves as the above-mentioned firewall and a client node on the Internet; 2.) using the shared private keys to establish mutual authentication between the gateway and the smart card; 3.) generating a session or temporary secret key for use in further communications between the gateway and the client node once communications have been established; and 4.) encrypting further communications using the session key.