PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 29/06 — A1

(11) International Publication Number: WO 00/59177

(43) International Publication Date: 5 October 2000 (05.10.00)

(21) International Application Number: PCT/GB00/01078

(22) International Filing Date: 22 March 2000 (22.03.00)

(30) Priority Data:

9907442.9	31 March 1999 (31.03.99)	GB
99305557.3	13 July 1999 (13.07.99)	GB

(71) Applicant *(for all designated States except US)*: BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY [GB/GB]; 81 Newgate Street, London EC1A 7AJ (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: WRIGHT, Trevor [GB/GB]; 15 Ditchingham Grove, Rushmere St. Andrew, Ipswich, Suffolk IP5 1WE (GB). TEDESCHI, Nigel [GB/GB]; 32 Wolton Road, Kesgrave, Ipswich, Suffolk IP5 2YT (GB).

(74) Agent: GARRISON, Christopher, Sinclair; BT Group Legal Services, Intellectual Property Dept., 8th floor, Holborn Centre, 120 Holborn, London EC1N 2TE (GB).

(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, 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, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, 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 the receipt of amendments.

(54) Title: SERVER COMPUTER FOR GUARANTEEING FILES INTEGRITY

(57) Abstract

The problem of the vulnerability of electronic content stored on server computers to alteration by unauthorised third parties is one which has become much exacerbated with the advent of the Internet and the World Wide Web. Present day approaches, including approaches based on digital signature techniques, allow for the checking of content transmitted over communications networks to, for example, client computers, to establish if tampering by unauthorised third parties has occurred. Such approaches all suffer from the disadvantage that any content which has been tampered with is still transmitted over the network to the client computer before such a check takes place. According to the invention however, a server computer storing computer files, each computer file having an associated unique digital signature, receiving requests for access to one or more such computer files, only allows access to the or each computer file if their associated digital signatures are valid. Thus, if a computer file has been tampered with by an unauthorised third party, the digital signature associated with that computer file will prove to be invalid when checked and the server computer will not serve the computer file at all. In this way, a computer file that has been tampered with can never leave the server computer, much improving the security of the stored computer files.