9805442
IPOS copy

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32

A1

(11) International Publication Number: WO 97/39553

(43) International Publication Date: 23 October 1997 (23.10.97)

(21) International Application Number: PCT/US97/04025

(22) International Filing Date: 14 March 1997 (14.03.97)

(30) Priority Data:
08/634,068 17 April 1996 (17.04.96) US

(71) Applicant *(for all designated States except US)*: INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

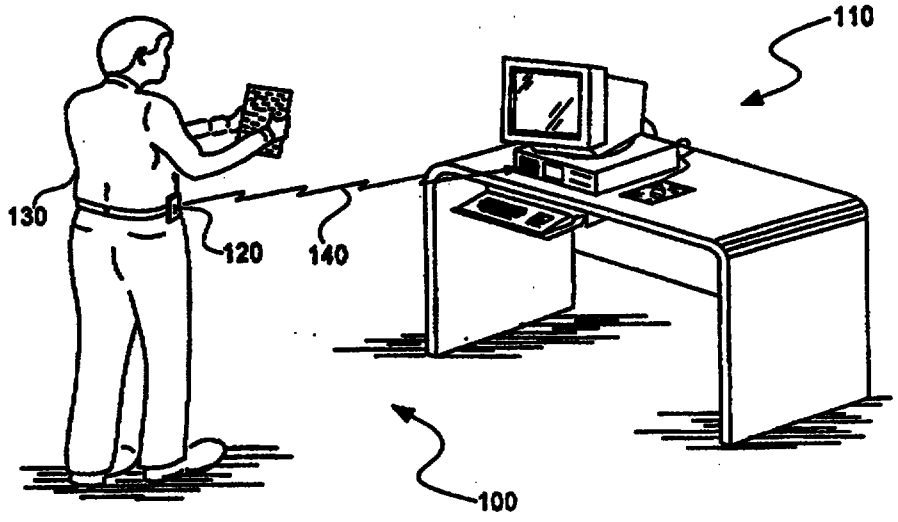
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: DAVIS, Derek, L. [US/US]; 4509 E. Desert Trumpet Road, Phoenix, AZ 85044 (US). SMITH, Lionel [US/US]; 23412 Via del Arroyo, Queen Creek, AZ 85242 (US).

(74) Agents: TAYLOR, Edwin, H. et al.; Blakely, Sokoloff, Taylor & Zafman L.L.P., 1279 Oakmead Parkway, Sunnyvale, CA 94086 (US).

(81) Designated States: AL, AM, AT, AT (Utility model), AU (Petty patent), AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: AN AUTHENTICATION SYSTEM BASED ON PERIODIC CHALLENGE/RESPONSE PROTOCOL



(57) Abstract

A wireless authentication system to control an operating state of a node such as a computer, door control mechanism or any multistate product based on the proximity of an authorized user to the node. The wireless authentication system comprises a security device implemented within the node (110) and a user authentication token ("token") in possession of the authorized user. A Challenge/Response protocol (140) is configured between the security device and the token (120). The first successful Challenge/Response message exchange between the security device and the token (120) places the node (110) in an operational state allowing the authorized user access to the contents and/or networked resources of the node (110). Later Challenge/Response message exchanges are set to occur periodically to check whether the authorized user possessing the token has left the node (110) unattended thereby causing the node (110) to be placed in a non-operational state.